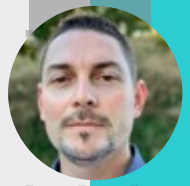
FORTINET

FortiWeb

Web Application and API Security

Sébastien BEAL

CISSP / Team Leader Channel System Engineering



Web Applications are Under Attack

Threat actors are actively seeking to exploit vulnerable web applications

Overall, the IPS detections shown reflect several general trends we've seen for some time now: web servers, content management systems (CMS), and Internet of Things (IoT) devices.

– **FortiGuard Labs Global Threat Landscape Report, 1H 2021**

> *…the IPS triggers racking up the highest volume were HTTP.Server.Authorization.Buffer.Overflow and HTTP.URI.Java.Code.Injection, while HTTP.Header.SQL.Injection and HTTP.URI.SQL.injection were detected by the largest number of organizations.*

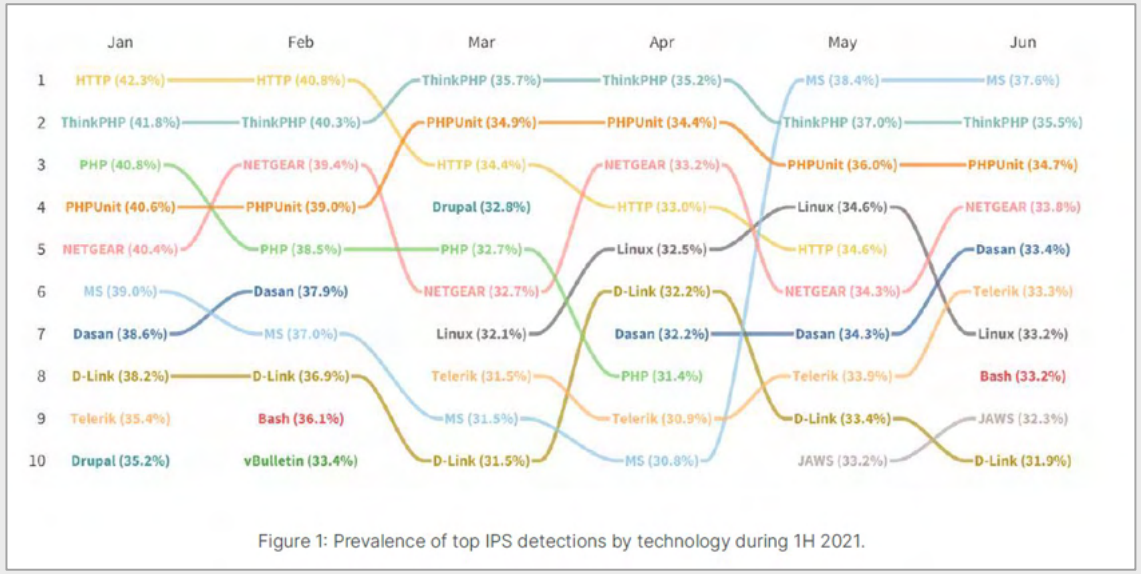


Figure 1: Prevalence of top IPS detections by technology during 1H 2021.

The Evolution of Web Applications for Critical Line of Business Functions Motivates Threat Actors

“Line-of-business application” support the critical workflows that support your business, including:

- Ecommerce
- Supply chain management
- Business intelligence
- Travel
- Payroll

These web applications provide access to your organization’s most critical data:

- Customer PII
- Employee PII
- Financial data
- Competitive intelligence

Cyber criminals motivated by financial gain, and state-sponsored threat actors motivated by geopolitics, have the resources to target the critical data your web applications rely on.

As Organizations Push Out Application Changes at a Rapid Pace…

48%

of the organizations have 100 or more unique applications in their environment

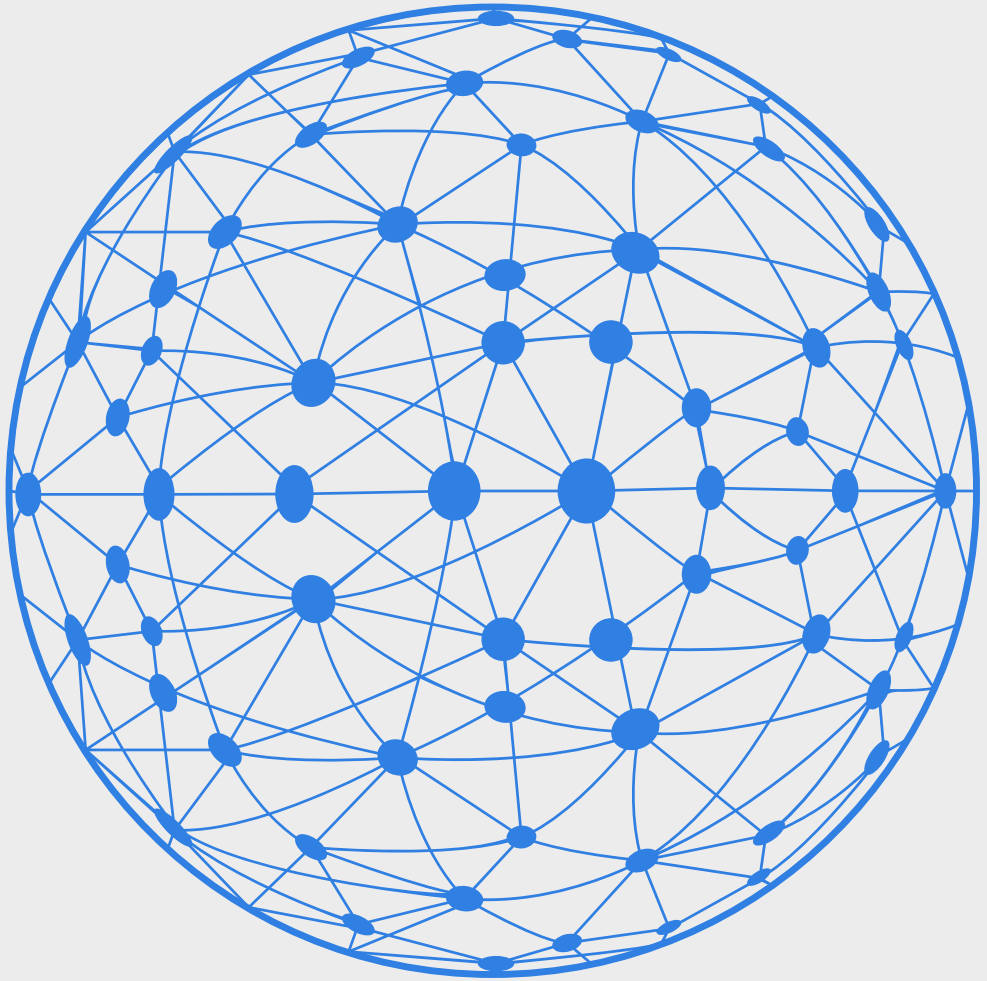
On average, companies publish

25

Software updates into production on a monthly basis

For the full report, go to https://go.fortinet.com/global-lp/aws-app-security-report

The Attack Surface for Web Applications Evolves



Exploits

including OWASP Top 10

Advanced Threats

including zero-day attacks

Bot Attacks

including credential stuffing, content scraping

API Attacks

including attacks that extract bulk data

And Threat Actors have Expanded their Toolkits to Target the Expanded Attack Surface

Automated Attacks

Malware

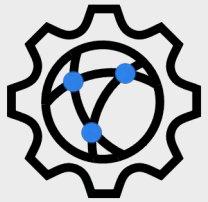
Advanced Threats

API Exploits

Data Exfiltration

Zero Day Attacks

Application Layer Attacks

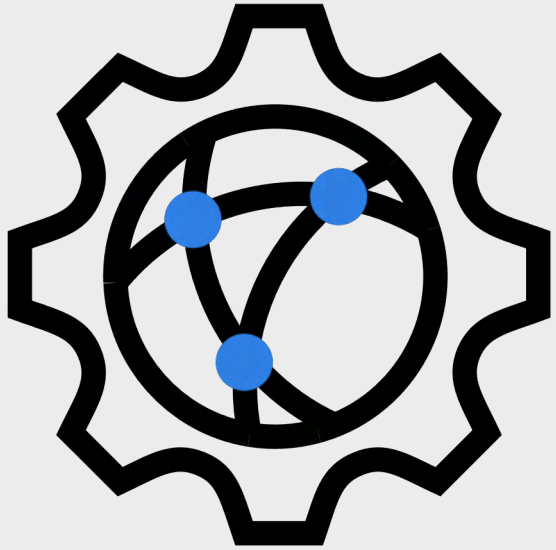


FortiWeb

Web Application and API Protection

Key Web Application & API Security Use Cases

Application Security

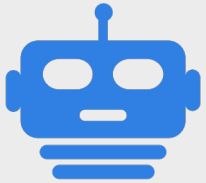


FortiWeb

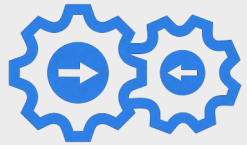
Web Application Security

Regulatory Compliance

SOC Operations

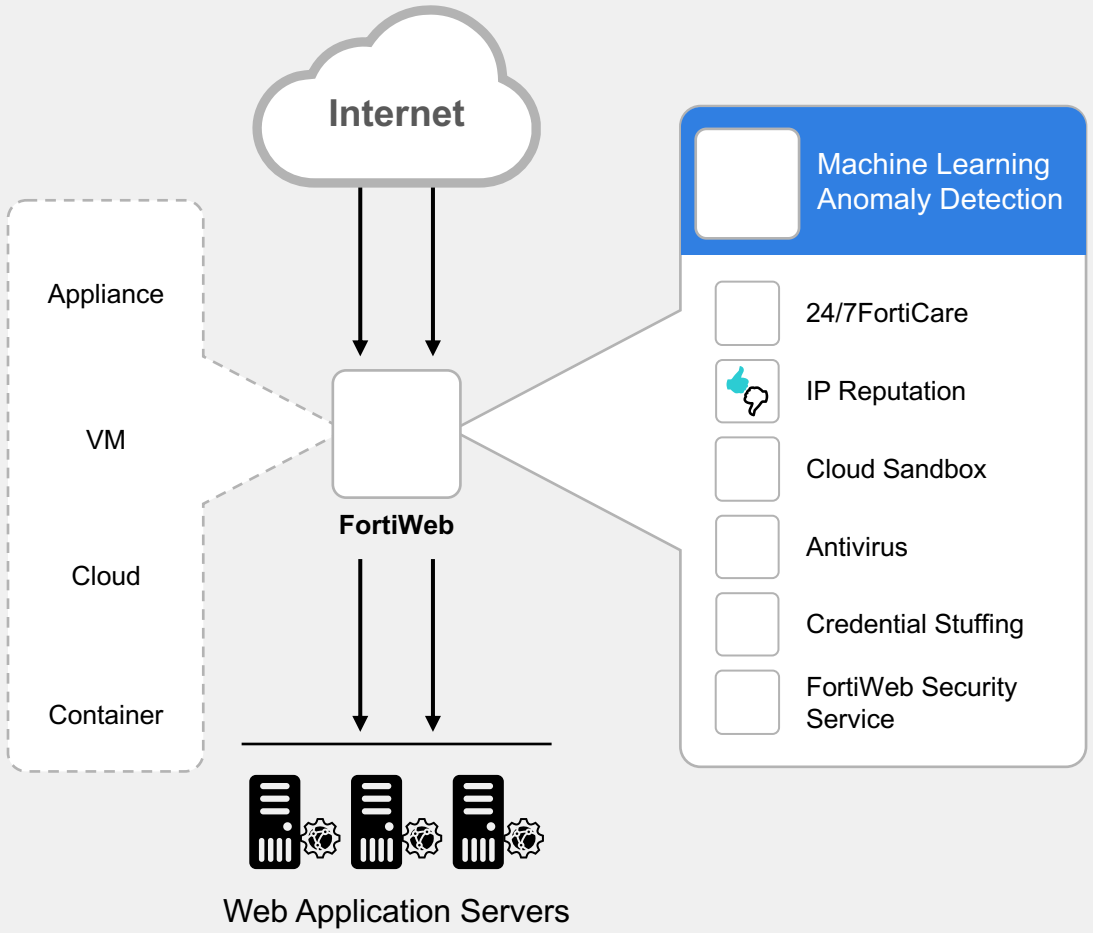


Bot Defense



Protect Internet-facing APIs

Web Application Security



1. Web Application Security

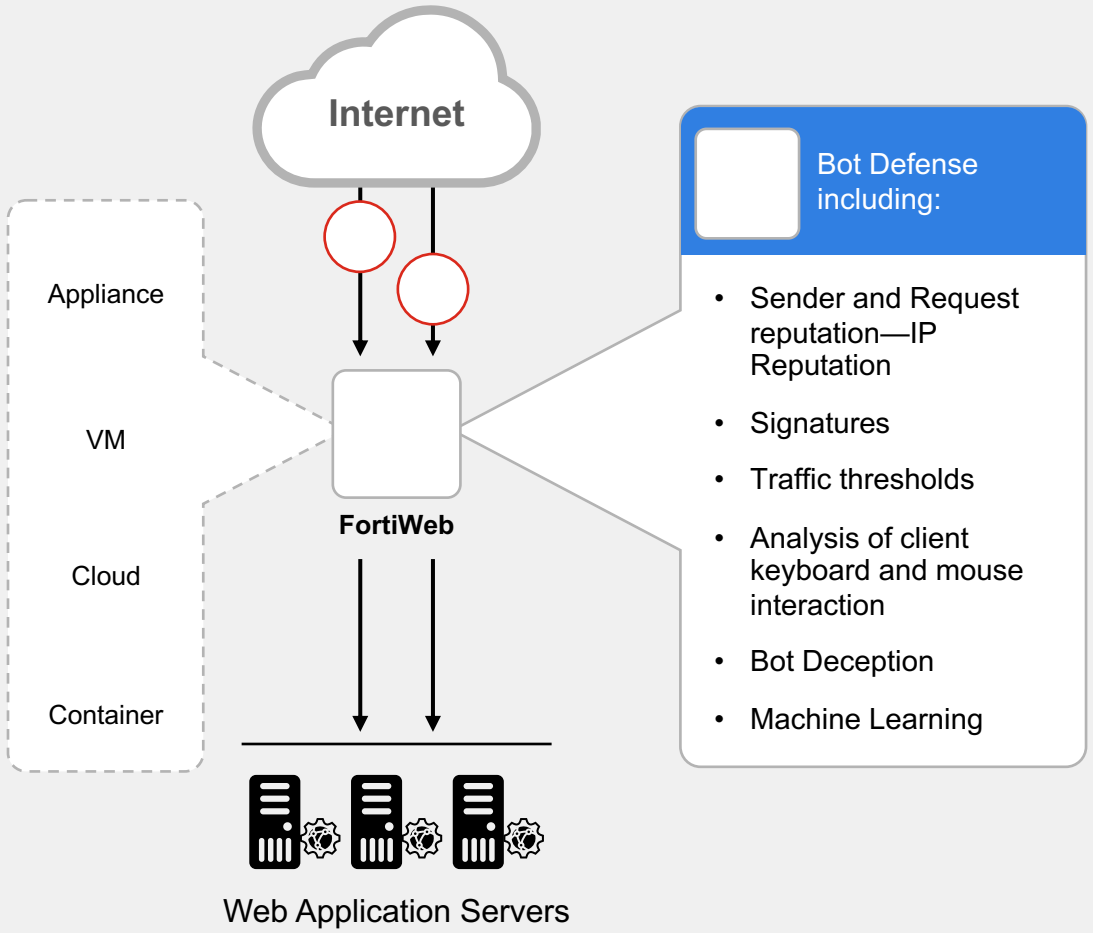
Protect from OWASP top 10 and other known threats as well as unknown threats.

ML Optimized Business Application Security

Protects against threats to web-based applications:

- Protect against known risks, including the OWASP Top 10
- Protection against unknown and zero-day threats
- Reduces administrative overhead by reducing false positives with machine learning

Bot Defense



2. Bot Defense

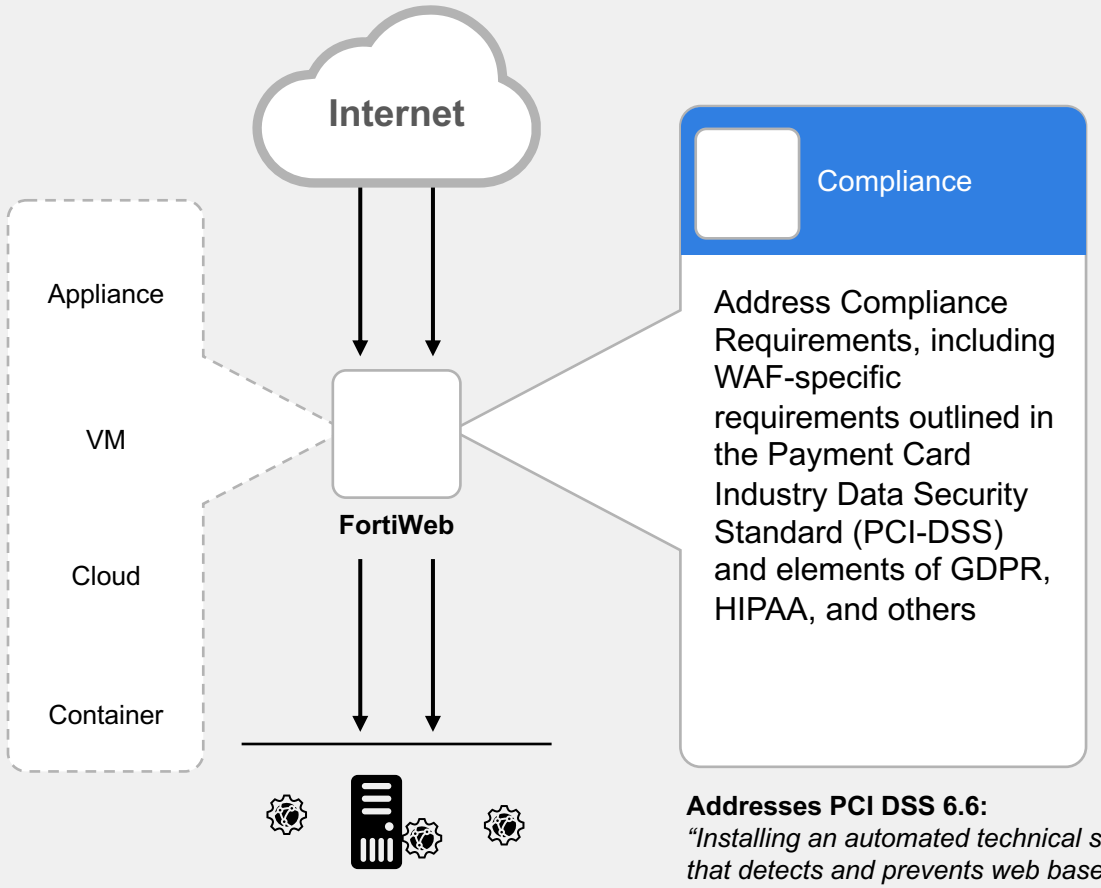
Block the full range of malicious bot activity (e.g., content scraping, denial of service, data harvesting, transaction fraud).

Advanced ML Powered Bot Detection

Protection of applications from bots:

- Blocks malicious bots without blocking users or interfering with legitimate bot activity such as search engines
- Reduce or eliminate reliance on user verification techniques that degrade the user experience such as ReCaptcha

Regulatory Compliance



Addresses PCI DSS 6.6:
"Installing an automated technical solution that detects and prevents web based attacks (for example, a web application firewall) in front of public facing web applications, to continually check all traffic."

3. Regulatory Compliance

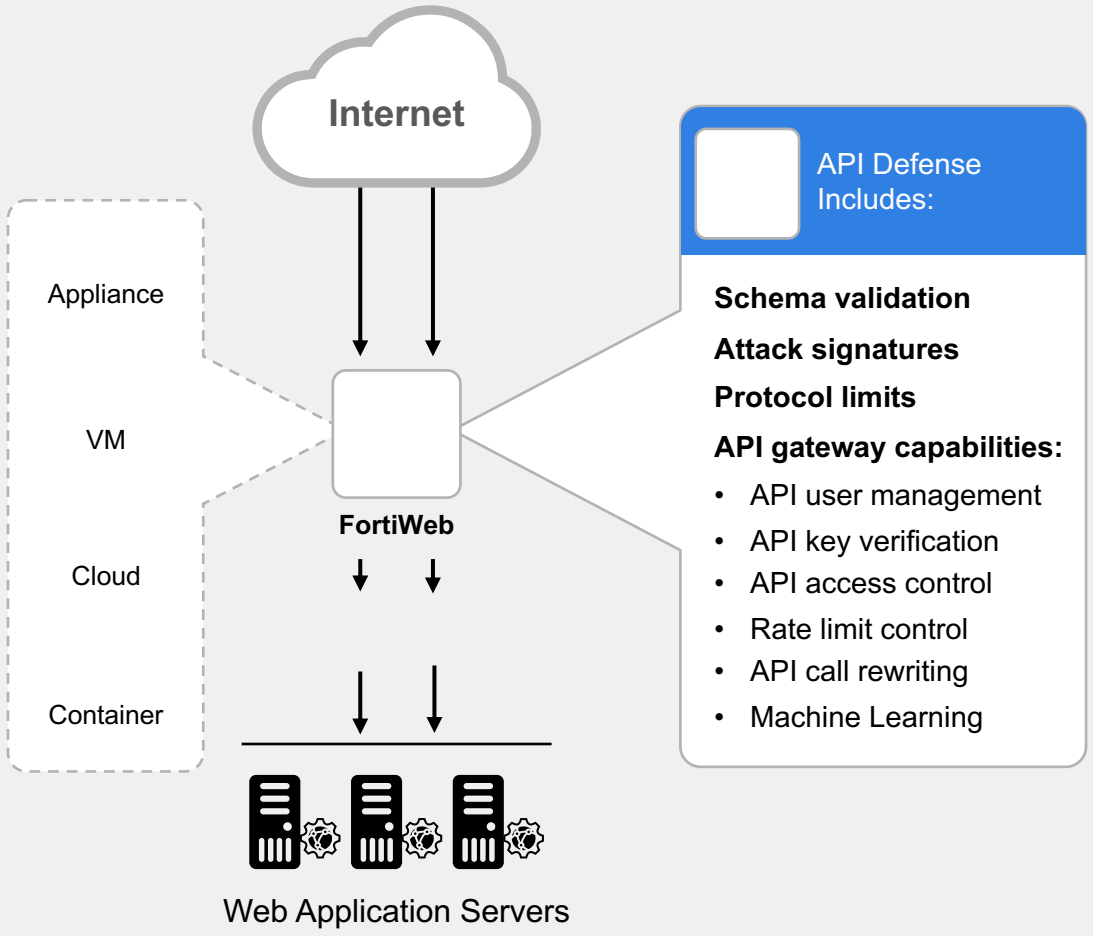
Address regulatory compliance requirements related to public-facing applications.

Meet Compliance Requirements

Address specific compliance controls for protection of web-based applications:

- Protect against known risks, including common web threats such as those listed in the OWASP Top 10
- Address PCI-DSS 6.6 requirements
  - PCI DSS is mandated by credit card companies and applies to all entities that store, process or transmit cardholder data

Protect Internet-Facing APIs



4. Protect Internet-Facing APIs

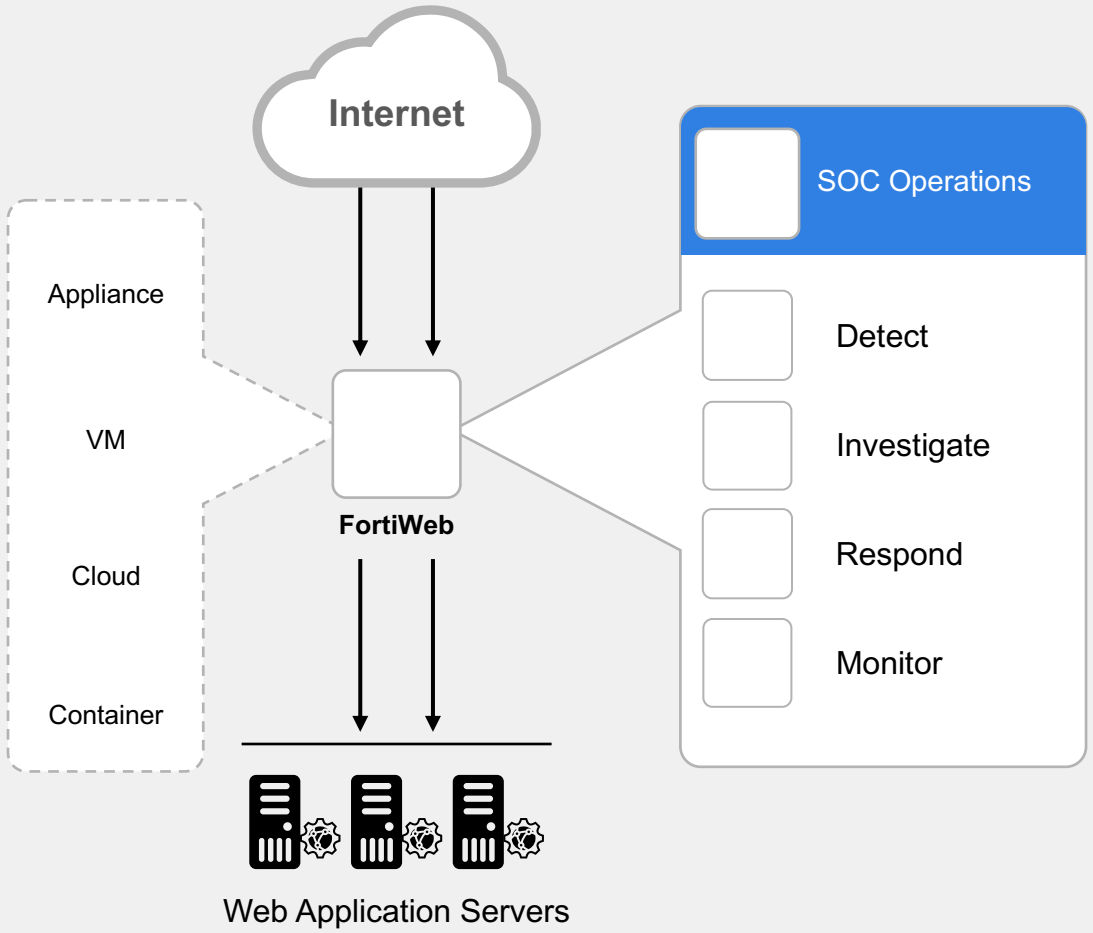
Protect the APIs that enable B2B communication and support your mobile applications.

Leverage ML to protect that APIs that support critical line-of-business capabilities

Advanced protection for APIs:

- Single point of access to APIs
- Hides internal API structure from potential attackers
- Delivers improved user experience for users on a wide range of devices without sacrificing security
- Machine Learning for API discovery and protection

SOC Operations



5. SOC Operations

Threat Analytics consolidates raw event data into a clear picture of the most important threats so that SOC analysts can prioritize mitigation for the most significant threats.

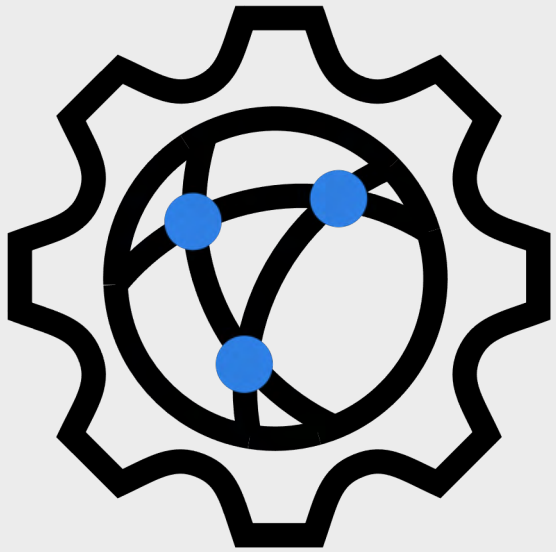
Leverage Threat Analytics to Highlight Actionable Threat Intel

Enable the SOC team to:

- Reduce administrative overhead by consolidating individual events into discreet threats, reducing manual analysis tasks
- Speed Investigations and enable rapid response
- Identify threats that require policy changes or additional monitoring
- Focus limited resources on mitigating the most important threats

FortiWeb Address the Key Web Application and API Security Use Cases

Application Security



FortiWeb

1. Web Application Security

Protect from OWASP top 10 and other known threats as well as unknown threats.

ML Optimized Business Application Security

2. Bot Defense

Block the full range of malicious bot activity (for example content scraping, denial of service, data harvesting, transaction fraud).

Advanced ML Powered Bot Detection

3. Regulatory Compliance

Address regulatory compliance requirements related to public-facing applications.

Meet Compliance Requirements

4. Protect Internet-facing APIs

Protect the APIs that enable B2B communication and support your mobile applications.

Leverage ML to Protect APIs That Support Critical Line-of-Business Capabilities

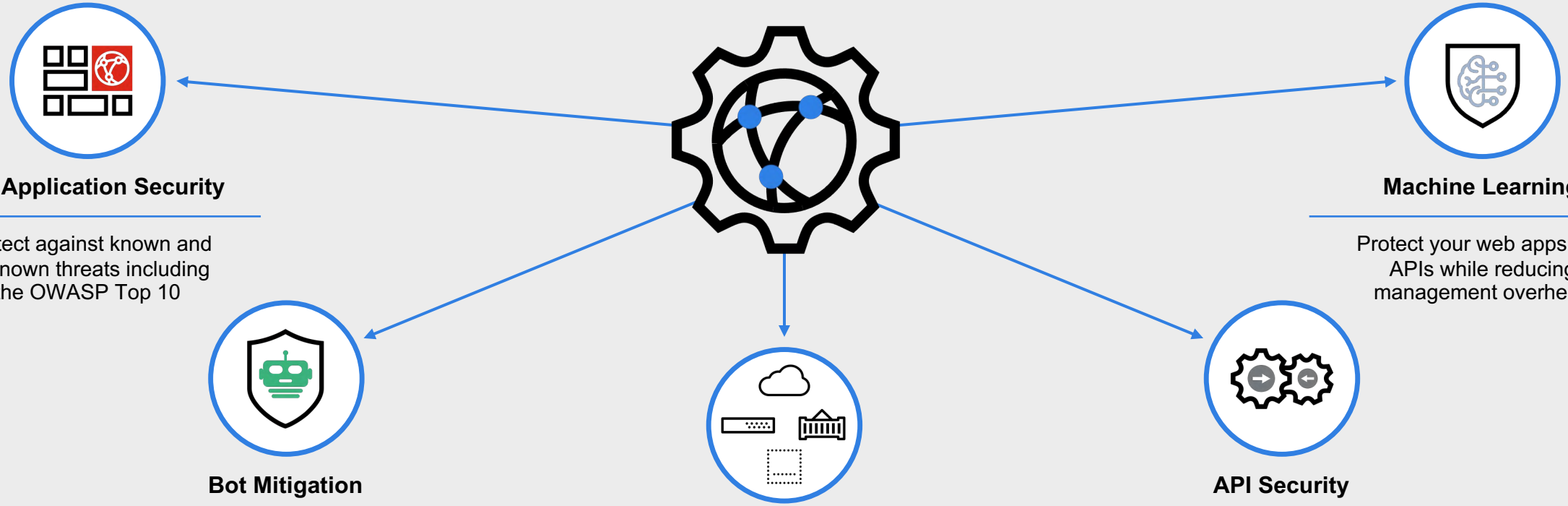
5. SOC Operations

Threat Analytics consolidates raw event data into a clear picture of the most important threats so that SOC analysts can prioritize mitigation for the most significant threats.

Leverage Threat Analytics to Highlight Actionable Threat Intel

FortiWeb Web Application Firewall Offers

Web Application and API Protection



Web Application Security

Protect against known and unknown threats including the OWASP Top 10

Machine Learning

Protect your web apps and APIs while reducing management overhead

Bot Mitigation

Block the full range of malicious bot activity (e.g., content scraping, denial of service, data harvesting, transaction fraud)

Flexible Deployment Options

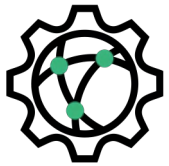
Protect any application, anywhere with flexible deployment options: Appliances, VM, container, or WAF as a Service

API Security

Protect the APIs that enable B2B communication and support your mobile applications

Powered by Cloud Delivered Threat Intelligence

FortiGuard Services

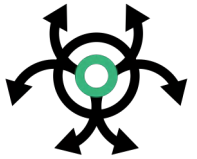


Web Application Security

IP Reputation

Sandbox

Anti-botnet



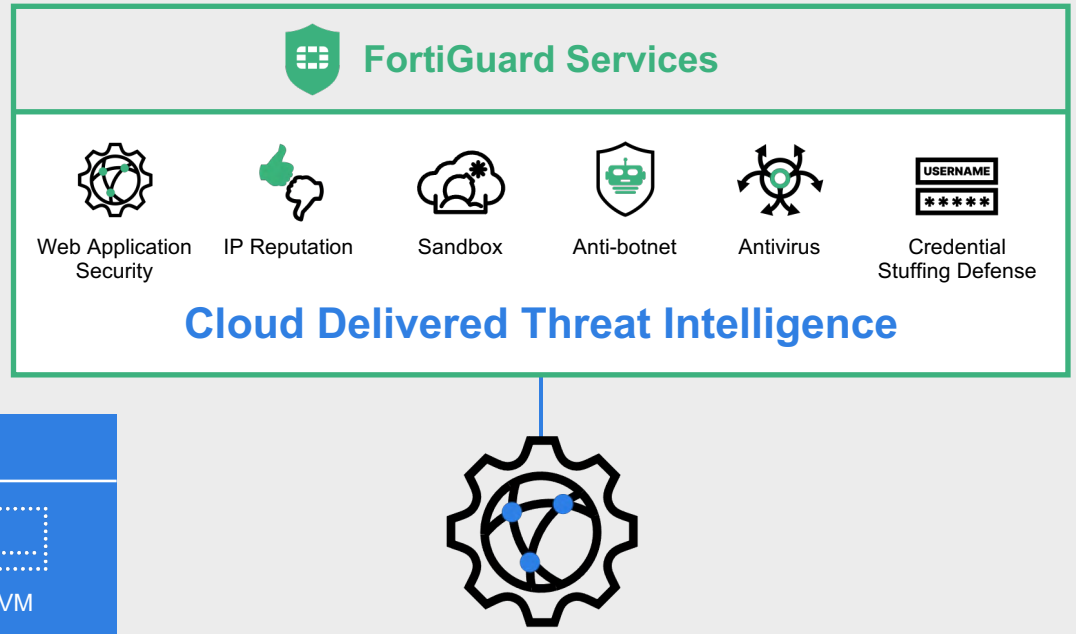
Antivirus

Credential Stuffing Defense

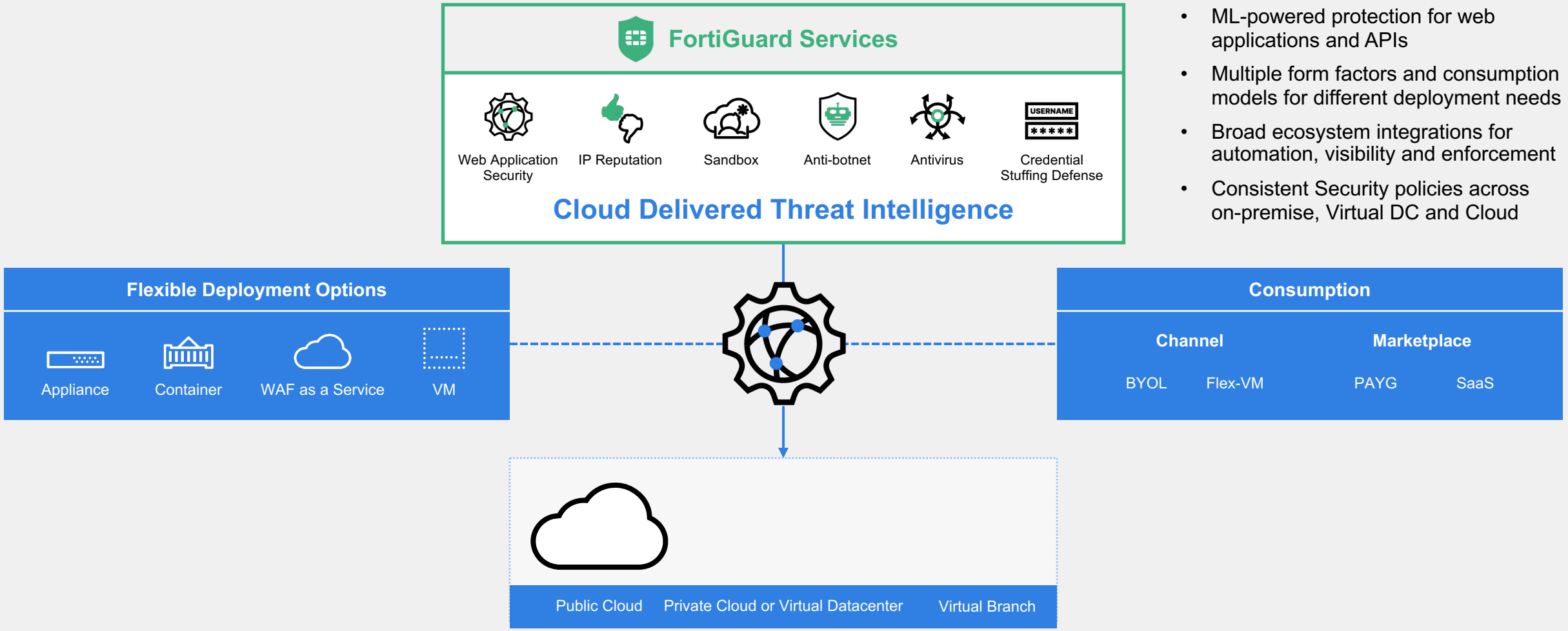
Cloud Delivered Threat Intelligence

Cloud Delivered Threat Intelligence

Flexible Deployment that Enable Protection Anywhere You Deploy



Flexible Consumption Models to Fit Your Business



- ML-powered protection for web applications and APIs
- Multiple form factors and consumption models for different deployment needs
- Broad ecosystem integrations for automation, visibility and enforcement
- Consistent Security policies across on-premise, Virtual DC and Cloud

FortiGuard Services for FortiWeb

SECURED BY
FortiGuard

WAF Security Service

- Application layer signatures
- Web application signature to prevent any web attack
- Machine learning threat models
- Malicious Bots

IP Reputation

- Protection for automated attacks and malicious sources
- DDoS, Phishing, Botnet, Spam, anonymous proxies and infected sources

Anti-malware

- Scan file uploads
- Regular and extended AV databases
- Protect the network against exploitable vulnerabilities

STANDARD SUBSCRIPTION

FortiSandbox Cloud

- FortiSandbox hosted by Fortinet
- Subscription based
- No separate sandbox required

Credential Stuffing Defense

- Identifies login attempts using stolen credentials from numerous sources
- Automatic updates
- Prevents unwanted access and defends against data breaches

Threat Analytics

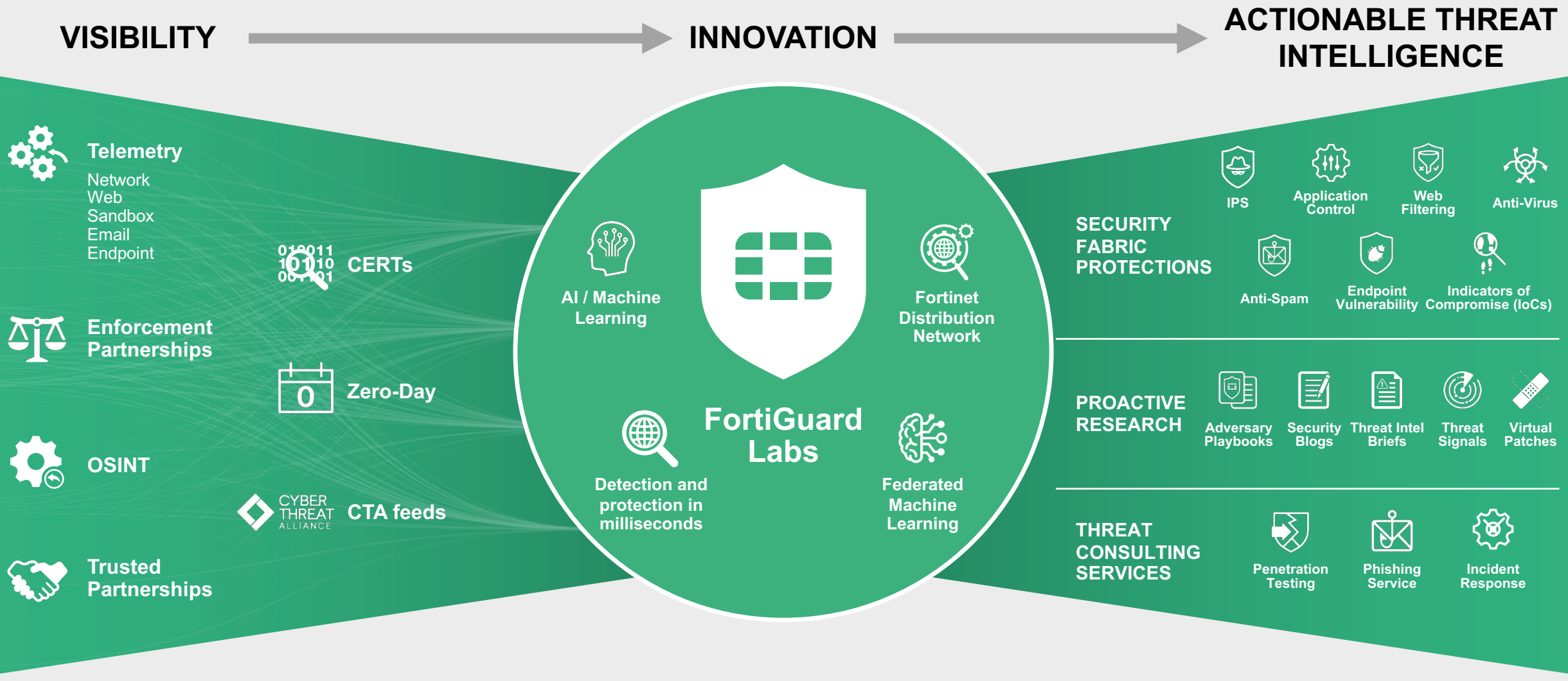
- AI-based threat analytics
- Identifies common characteristics and patterns and groups them into meaningful security incidents
- Incident risk prioritization

ADVANCED SUBSCRIPTION

Comprehensive WAF Security

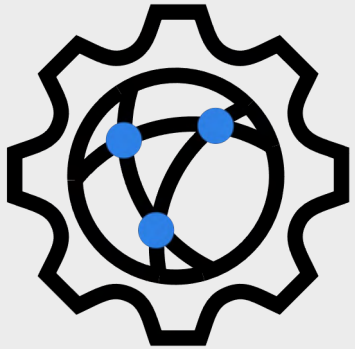
A multi-layer approach to protection web applications

Actionable Threat Intel From FortiGuard Labs



Threat Intelligence Lays the Foundation

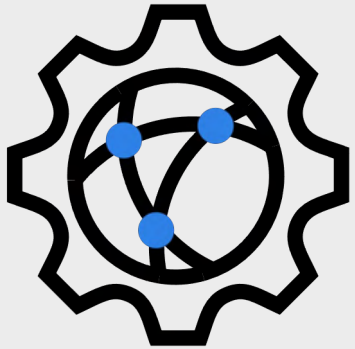
ATTACKS/THREATS	
BOTNETS, MALICIOUS HOSTS, ANONYMOUS PROXIES, DDOS SOURCES	**IP REPUTATION**
APPLICATION LEVEL DDOS ATTACKS	**DDOS PROTECTION**
IMPROPER HTTP RFC	**PROTOCOL VALIDATION**
KNOWN APPLICATION ATTACK TYPES	**ATTACK SIGNATURES**
VIRUSES, MALWARE, LOSS OF DATA	**ANTIVIRUS/DLP**



FortiWeb leverages threat intel from FortiGuard Labs to create signatures and block known malicious sources.

Fortinet Security Fabric Integration

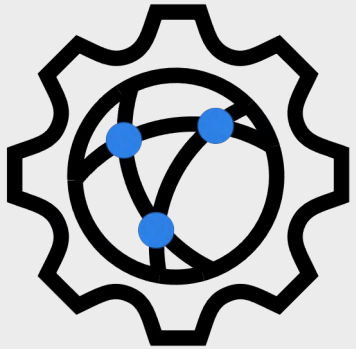
ATTACKS/THREATS	
BOTNETS, MALICIOUS HOSTS, ANONYMOUS PROXIES, DDOS SOURCES	IP REPUTATION
APPLICATION LEVEL DDOS ATTACKS	DDOS PROTECTION
IMPROPER HTTP RFC	PROTOCOL VALIDATION
KNOWN APPLICATION ATTACK TYPES	ATTACK SIGNATURES
VIRUSES, MALWARE, LOSS OF DATA	ANTIVIRUS/DLP
FORTIGATE AND FORTISANDBOX ATP DETECTION	FABRIC INTEGRATION



Integration with Fortinet Security Fabric components, including FortiGate and FortiSandbox, delivers enhanced ATP detection.

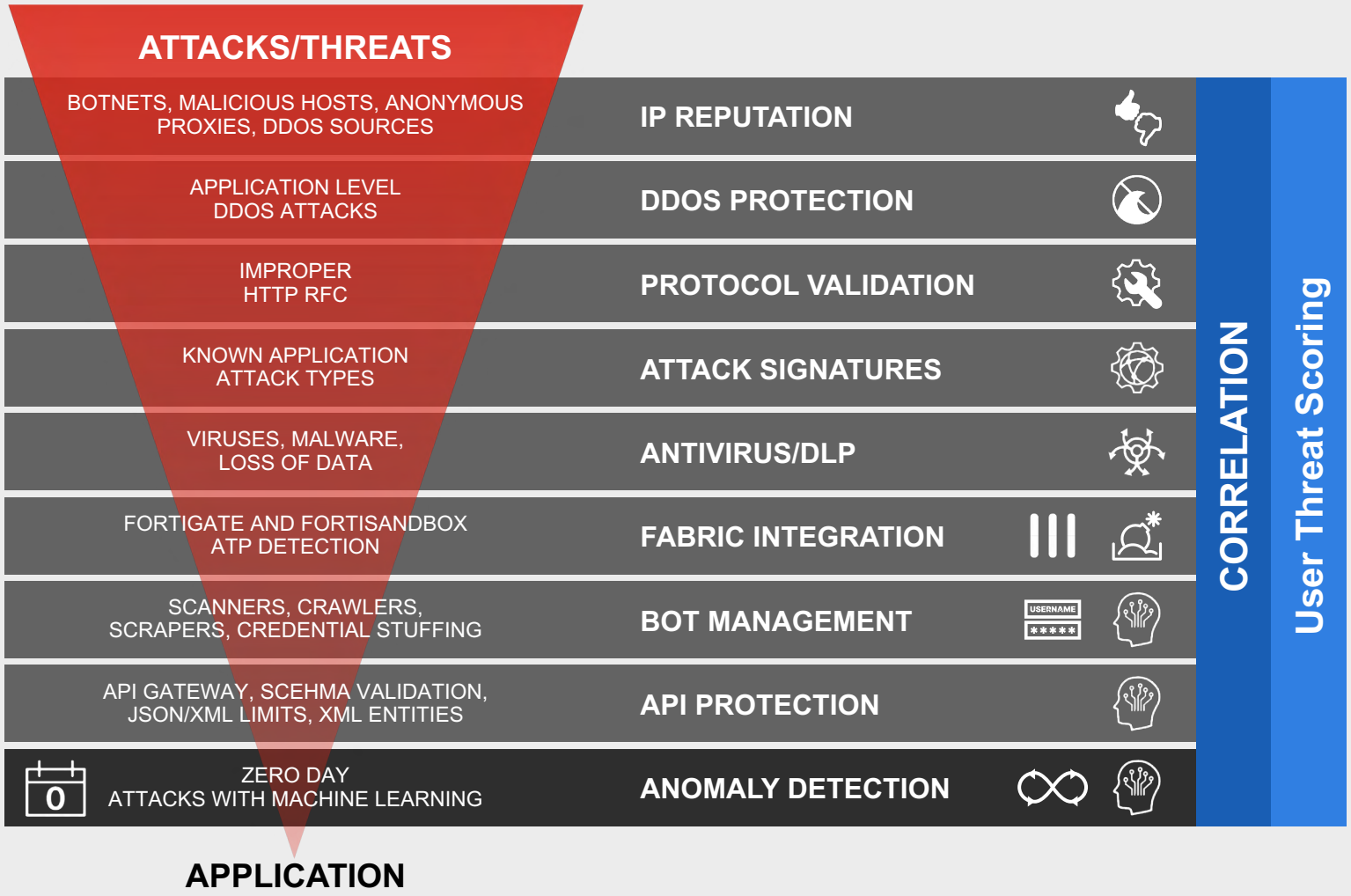
Bot Management and API Protection

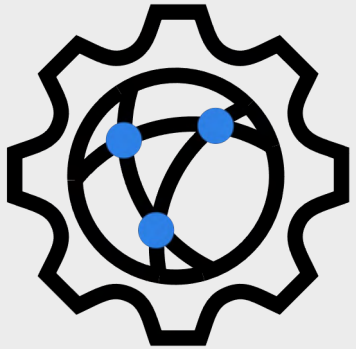
ATTACKS/THREATS	
BOTNETS, MALICIOUS HOSTS, ANONYMOUS PROXIES, DDOS SOURCES	IP REPUTATION
APPLICATION LEVEL DDOS ATTACKS	DDOS PROTECTION
IMPROPER HTTP RFC	PROTOCOL VALIDATION
KNOWN APPLICATION ATTACK TYPES	ATTACK SIGNATURES
VIRUSES, MALWARE, LOSS OF DATA	ANTIVIRUS/DLP
FORTIGATE AND FORTISANDBOX ATP DETECTION	FABRIC INTEGRATION
SCANNERS, CRAWLERS, SCRAPERS, CREDENTIAL STUFFING	BOT MANAGEMENT
API GATEWAY, SCEHMA VALIDATION, JSON/XML LIMITS, XML ENTITIES	API PROTECTION



FortWeb adds additional Bot Management and API Protection capabilities to deliver a full Web Application and API Protection (WAAP) solution.

Machine Learning for Anomaly Detection

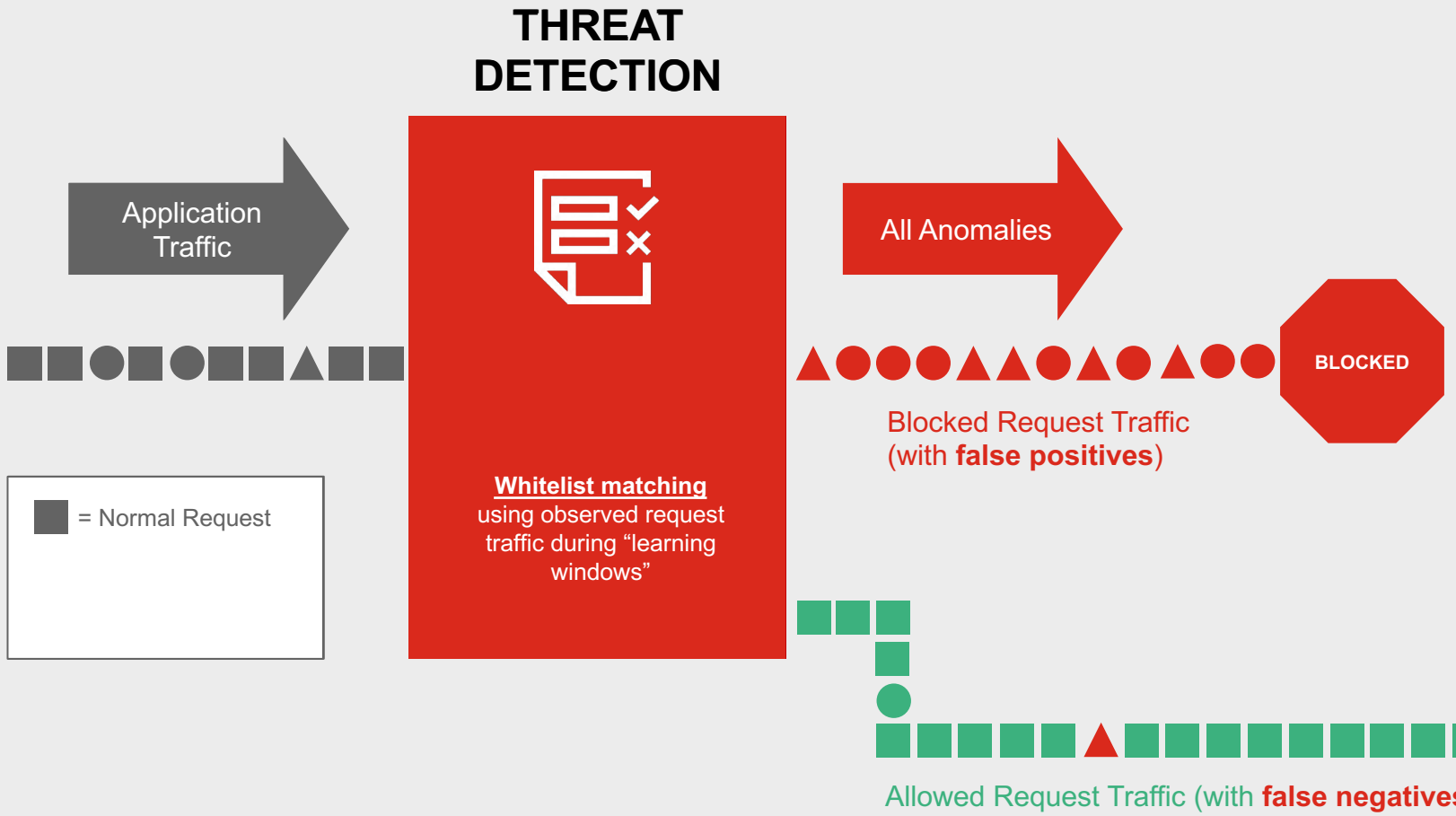




Machine Learning-based anomaly detection learns how your users interact with your application, delivering both improved threat detection and reducing the false positives that drive administrative overhead.

Why Machine Learning?

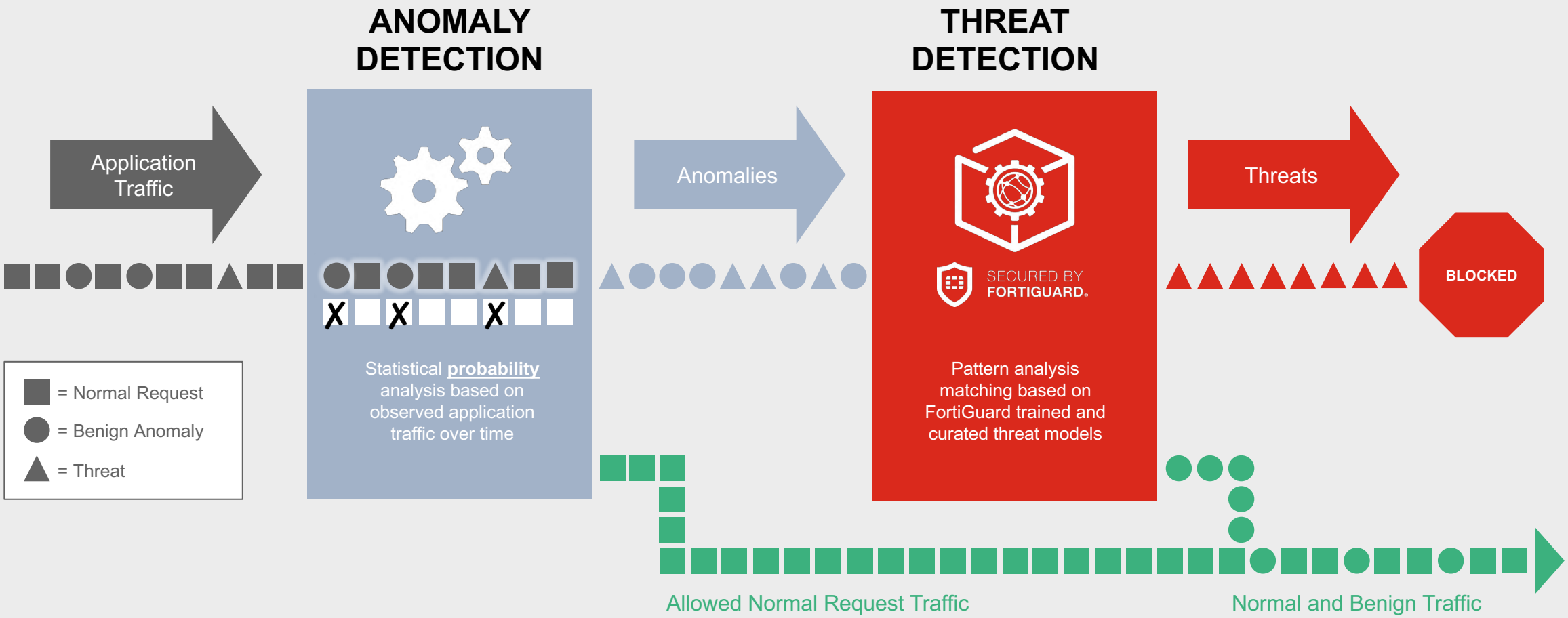
Traditional WAF Application Learning Detection



Known Issues/Limitations

- Blocking all anomalies leads to high false positives
- Accuracy requires labor intensive fine tuning
- Unobserved variations trigger anomalies
- Whitelisting characters used in attacks leads to threats evading detection
- Changes to application require relearning

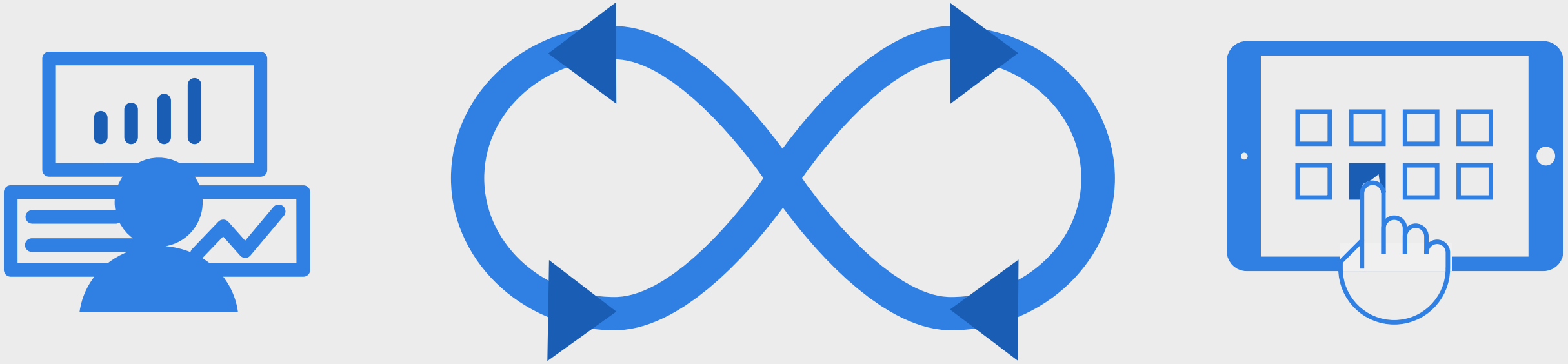
FortiWeb Employs Two Layers of Machine Learning



Reduce friction when deploying web applications!

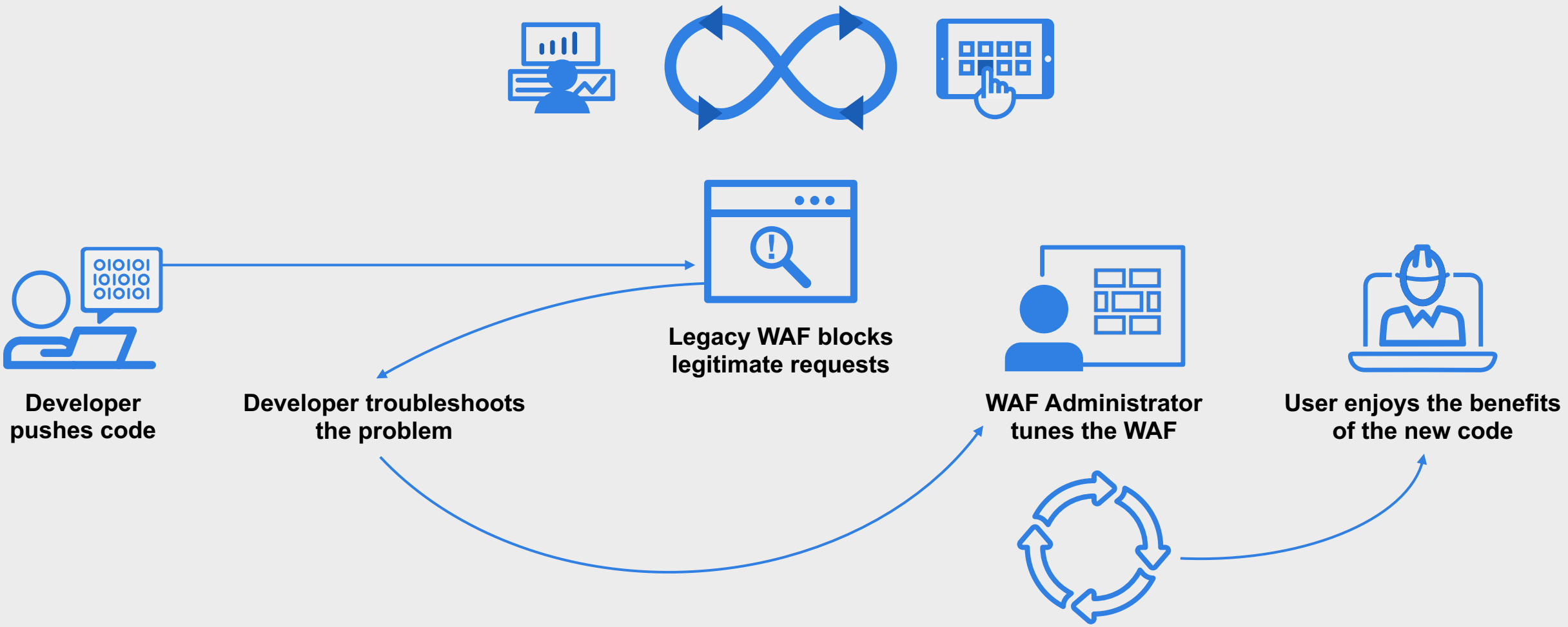
Why Machine Learning for Web Application Protection Matters for Customers

Reduce friction when deploying web applications



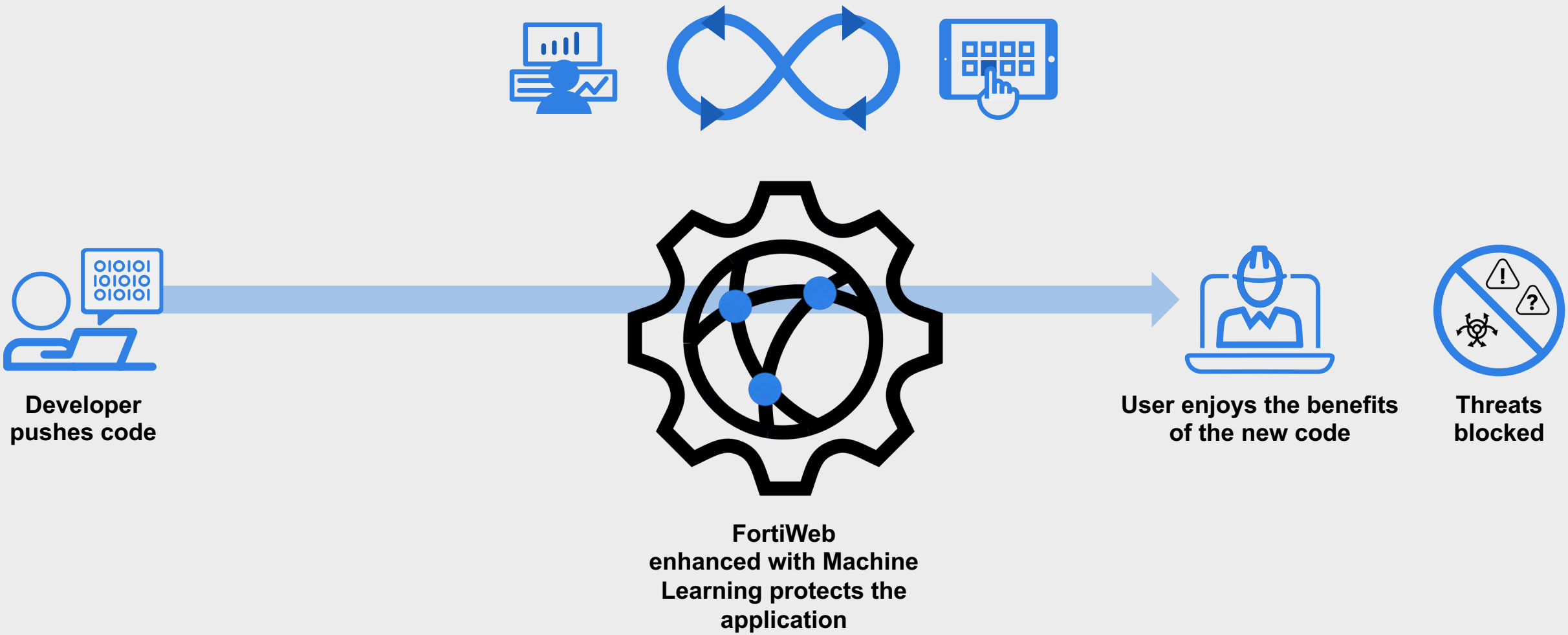
Continuous Integration and Continuous Deployment (CI/CD)

Old Fashioned WAFs Add Friction



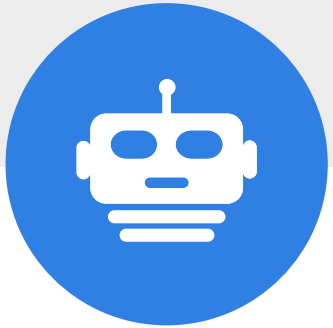
Machine Learning for Web Application Protection

FortiWeb with Machine Learning secures your application without slowing you down



Threat Analytics

Threat Analytics



The Rise of Bots and Attack Frameworks

Proliferation of applications and APIs mean more security alerts

Multi-layered Attack Strategies

Soc analysts are buried under a pile of informational alerts and false positives

Contextless Alerts

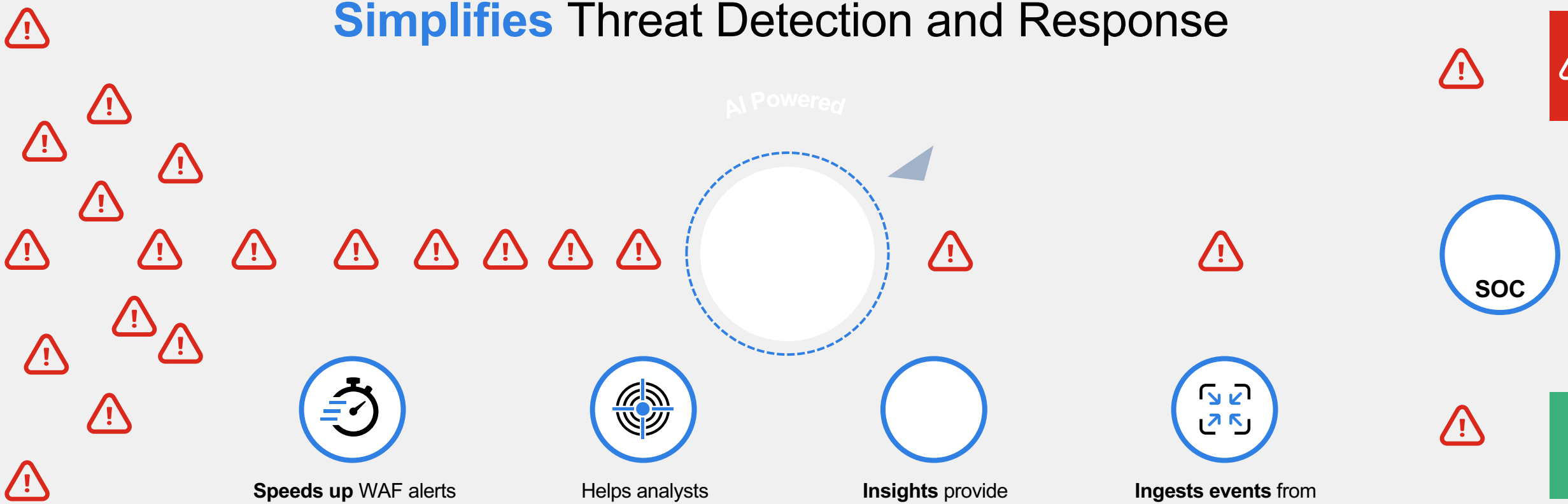
Events are not contextual making it harder to connect the dots and understand the real risk

Endless Stream of Meaningless Alerts

Security teams are not sure where to invest their time

FortiWeb Threat Analytics

Simplifies Threat Detection and Response



Speeds up WAF alerts security investigation

Helps analysts **focus** on the most important threats - alleviates alert fatigue

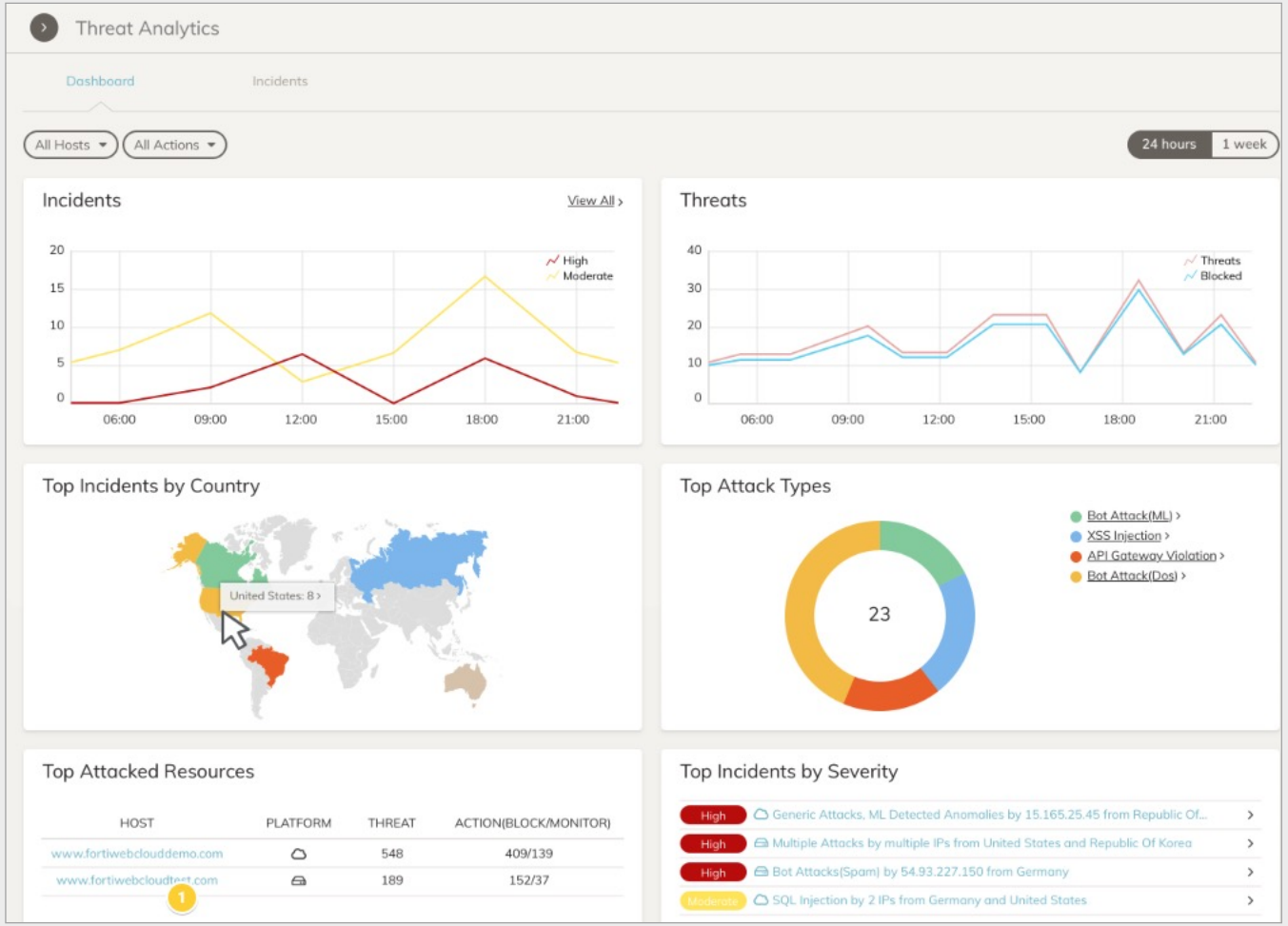
Insights provide suggestions to harden security based on findings

Ingests events from across your entire hybrid cloud environments

Threat Analytics

Identify the most important threats across the entire application attack surface

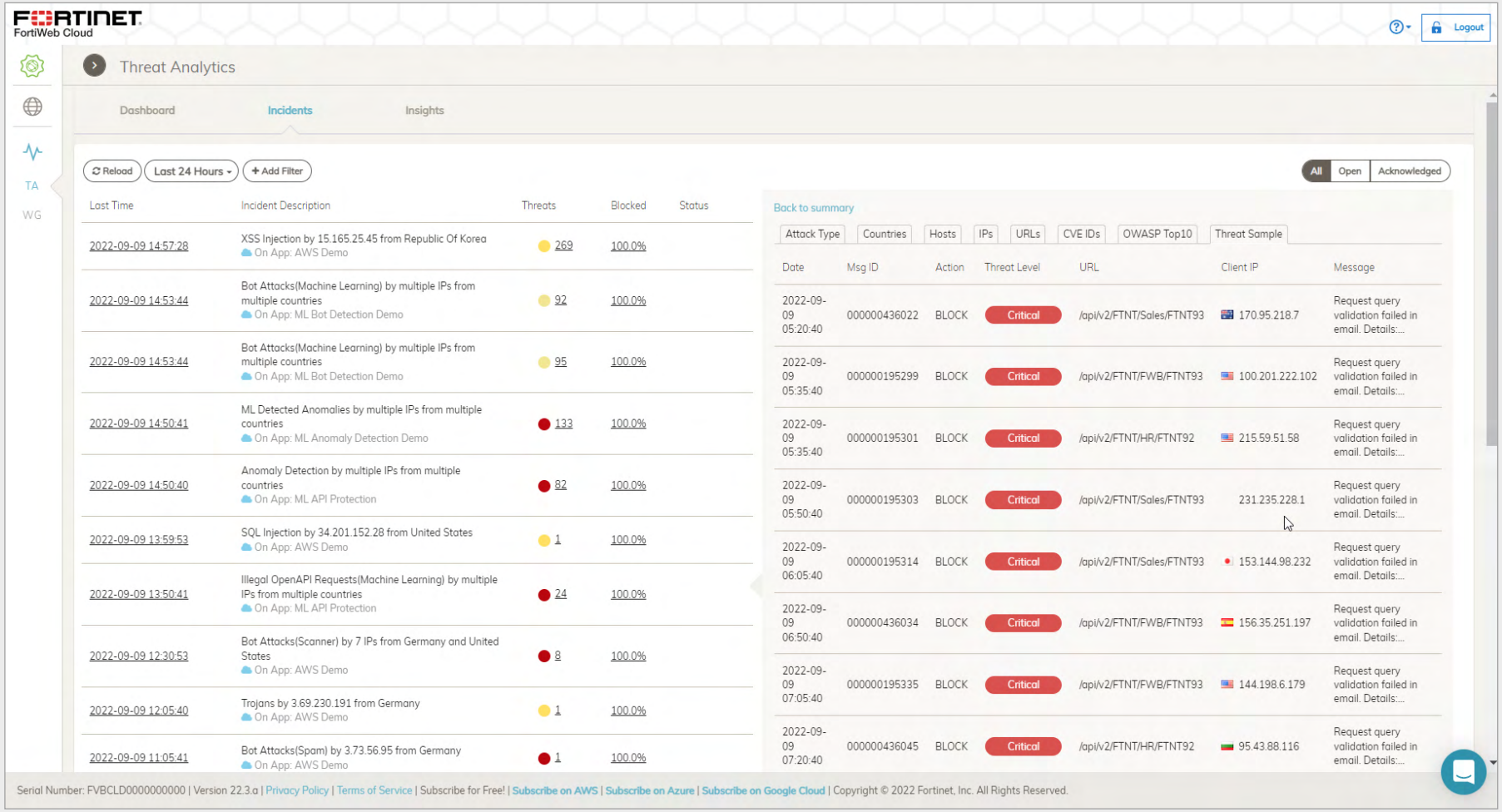
- Ingests events from all of your FortiWeb protected applications, including appliance, VM, and FortiWeb Cloud
- Identify attack campaigns across multiple web assets



Threat Analytics

Full attack details to enable:

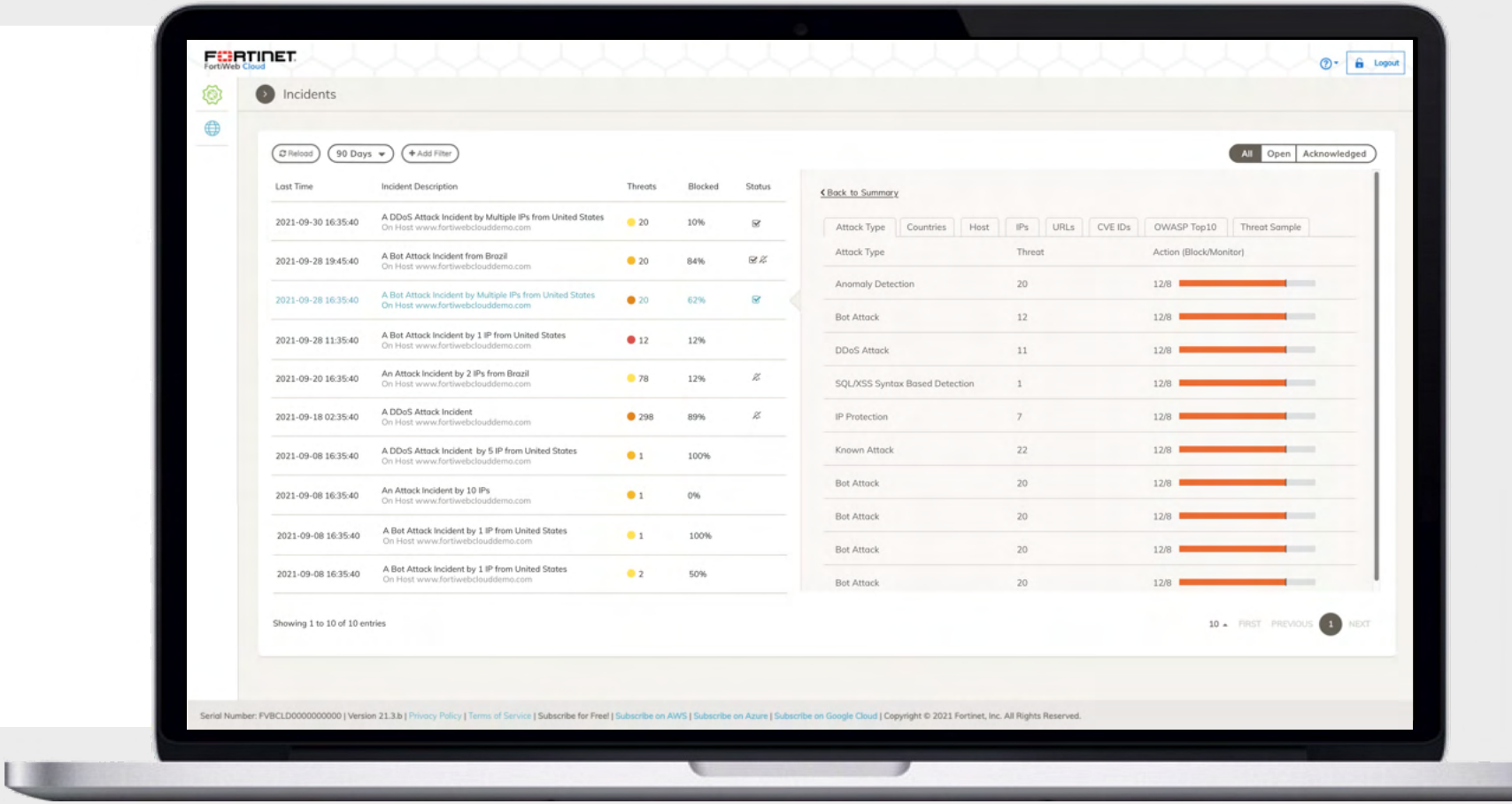
- Attack Type
- Countries
- Hosts
- IPs
- URLS
- CVE IDs
- OWASP Top 10
- Threat Sample



AI-Powered Threat Analytics

AI-powered threat analysis service that aggregates security alerts into clusters of narratives

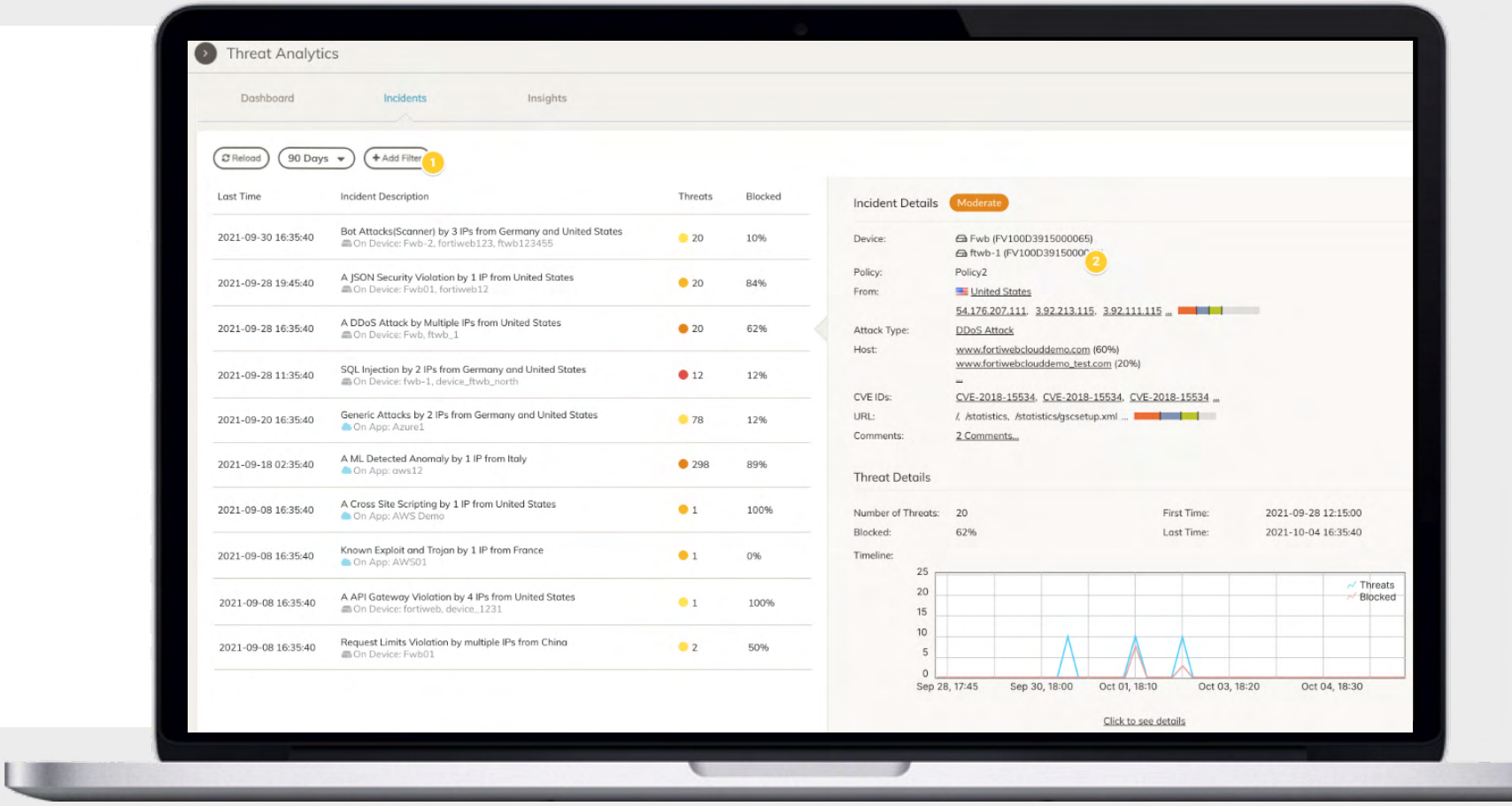
- Separate real threats from informational alerts and false positives
- Helps address alert fatigue
- Enrich incident context
- Actionable Insights
- Unified view—Cloud and onprem



Threat Analytics—Appliance Integration

View threats and patterns across the entire hybrid cloud

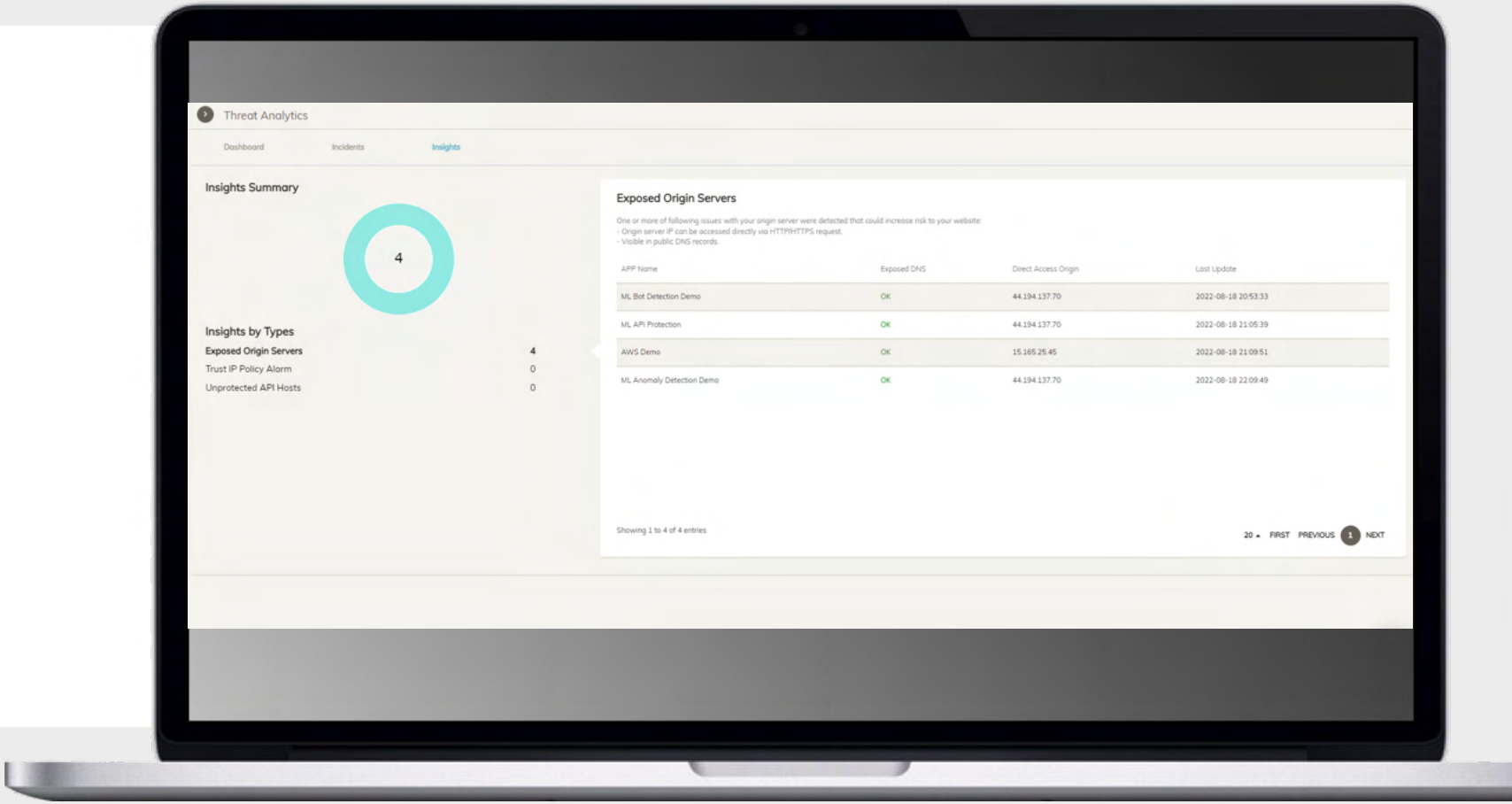
- Ingest events from FortiWeb HW/VM across hybrid cloud
- Identify advanced attacks across your entire web assets, wherever located
- Enhances Fortinet's telemetry and ability to deliver better security



Threat Analytics—Insights

Threat Analytics Insights identifies security issues

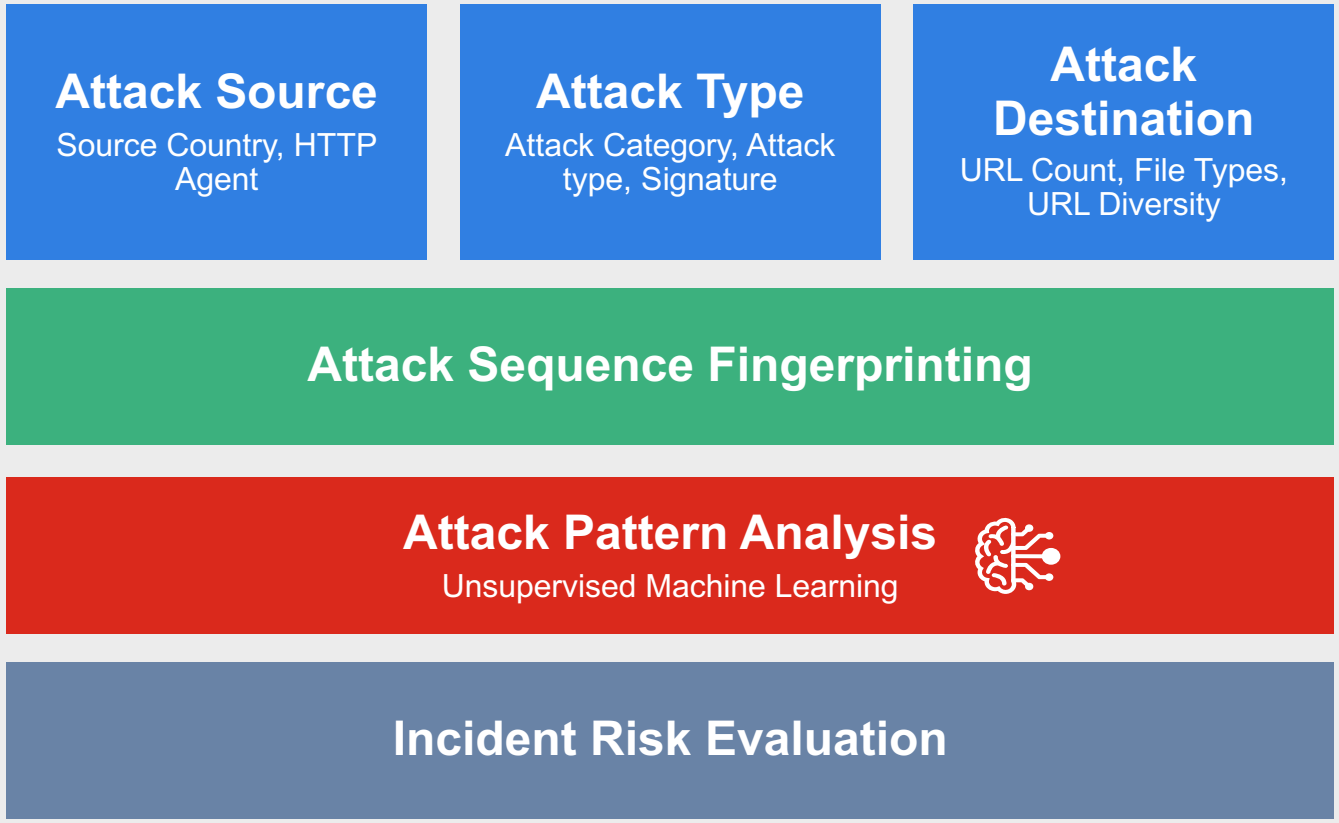
- Additional layer of configuration analysis
- Recommended actions
- Provide steps to remediate issues
  - Exposed origin servers
  - Trust IP policy alarm
  - Unprotected API hosts
  - WAF configuration alarm (22.3.b)
  - Fortinet Monitoring Service (22.3.b)



How it Works

FortiWeb Threat Analytics uses machine learning algorithms to identify attack patterns and aggregate them into security incidents across customer entire application assets.

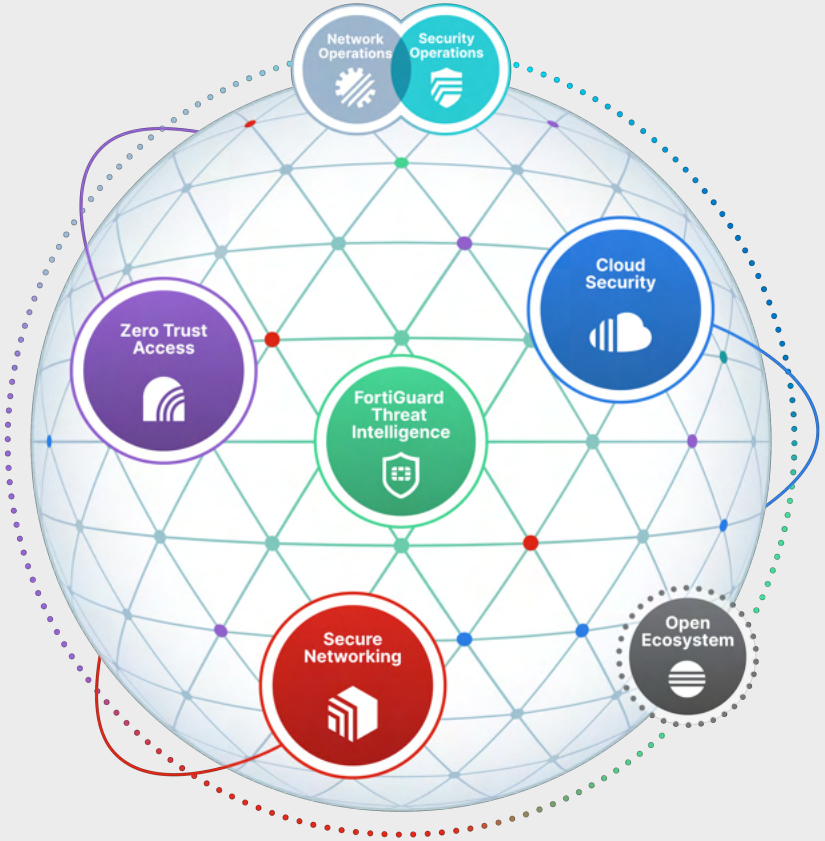
- Aggregate attacks into sequences
  - Same source and destination
  - No match for 60 min
- Create fingerprints for attack sequences
- Use ML to identify patterns in fingerprints
- Aggregate sequences into incidents
- Evaluate incident risk. Severity is impacted by:
  - Severity of every attack in incident
  - Number of attacks in incident
  - Variety of attack types



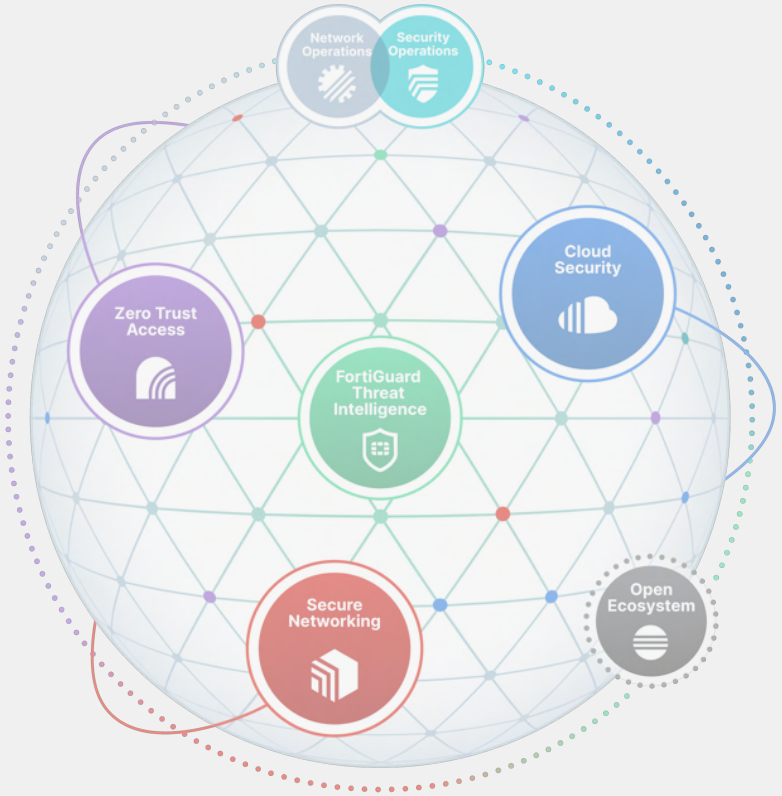
Security Fabric Integration

FortiWeb Security Fabric Integrations

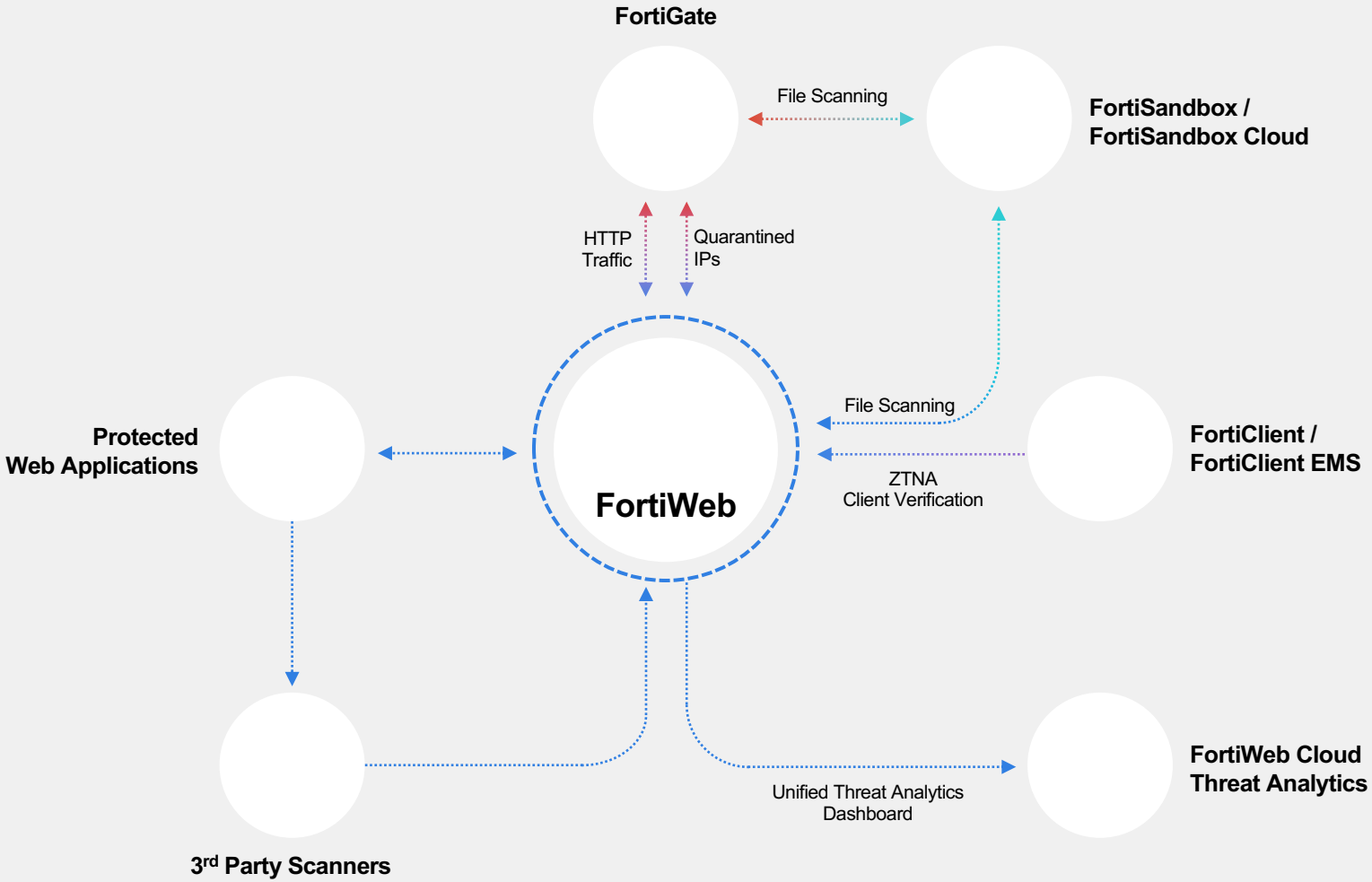
- FortiGate
  - Compromised user sharing with IP Polling
  - Simplified WCCP configuration
  - Threat Statistics
- FortiSandbox and FortiSandbox Cloud
  - File Scanning for unknown threats
  - APT protection
- FortiClient
  - ZTNA integration, verify client identity using client certificates.
- FortiWeb and FortiWeb Cloud
  - Shared threat analytics dashboard to identify the most critical threats
- Third Party Scanners (IBM, HPE, White Hat, and more)



FortiWeb Security Fabric Integrations



FortiWeb can be configured to join a Security Fabric through the root or downstream FortiGate



FortiWeb Web Application and API Security

Protection for Web Applications and APIs Everywhere You Deploy Them

Your applications and APIs

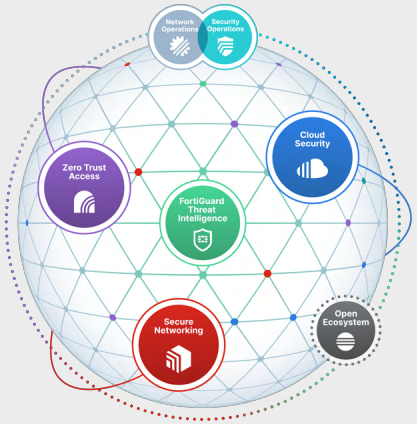
Deployed in the cloud or on-premise

Delivering Line of Business Capabilities

To your users, anywhere, from any device

Protected by FortiWeb's unique AI-powered detection engine, that minimizes false positives and reduces administrative overhead

Extending the protection of Fortinet's Security Fabric across your application attack surface



Deployment Flexibility

Maximum Deployment Flexibility

Delivering a full range of deployment options to support on-premise, hybrid, and pure cloud application deployments

Appliances

- 7 models
- 50 Mbps to 70 Gbps
- Support for 10/40GE

Virtual Machines

- 6 VM models
- CPU-based
- Perpetual and subscription licensing
- VMware, Hyper-V, Xen, Citrix Xenserver, KVM, Virtualbox

Public Cloud

- 4 VM models
- BYOL and on-demand
- AWS, Azure, Google Cloud, Oracle Cloud

SaaS

- Subscription
- Based on data consumption or throughput
- Hosted by Fortinet

Container

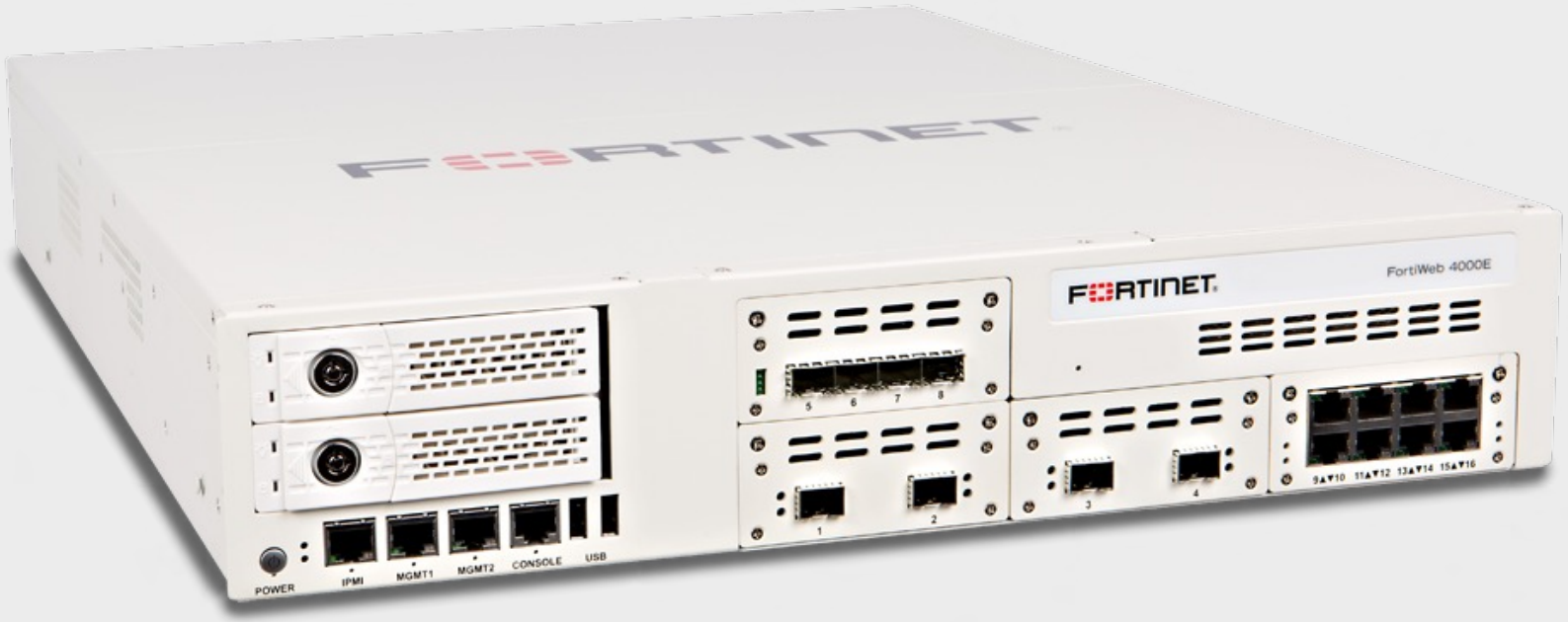
- 4 virtual appliances
- 25 Mbps to 2 Gbps
- Docker support

Partner Rules

- 5 packages
- Add on to AWS WAF
- Basic to complete OWASP Top 10 protection

FortiWeb Appliances and Virtual Machines

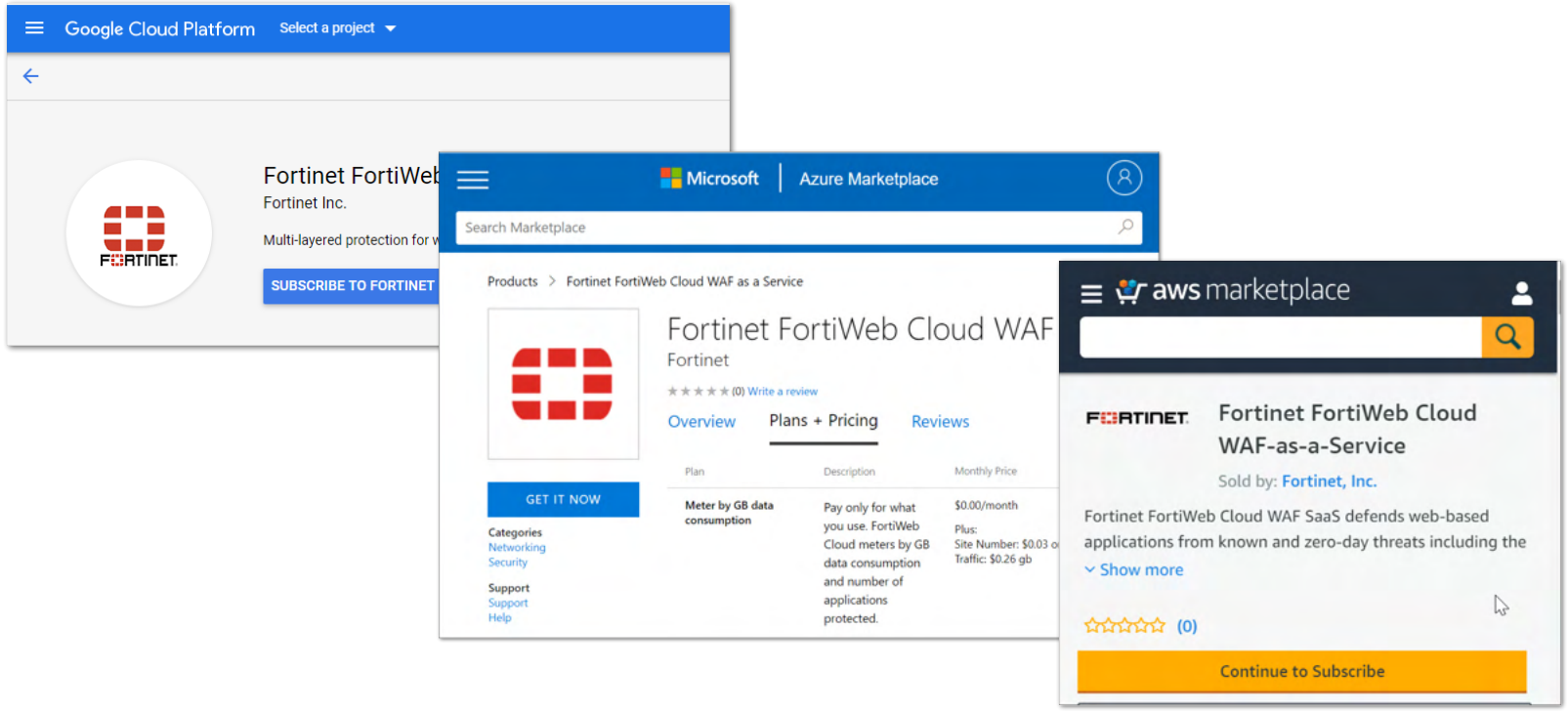
- 7 HW appliances and 6 VM models (50 Mbps to 70 Gbps)
- Virtual Machines available BYOL or PAYG for deployment in Public Cloud
- FortiGate, FortiSandbox, and FortiAnalyzer Integration



- Machine Learning threat detection
- API Discovery and Protection
- Layer 7 DDoS protection
- FortiGuard antivirus, IP reputation, FortiSandbox Cloud, Credential Stuffing Defense, and WAF signatures
- Exchange publishing and attachment scanning
- Native HTTP/2 WAF protection
- Central management/ADOMs
- REST API
- Included vulnerability scanner
- Virtual patching/third-party support
- Advanced false positive mitigation
- Advanced SQLi detection
- SSL offloading/compression
- SSO/authentication
- Layer 7 load balancing

FortiWeb Cloud

- Available on AWS, Azure, GCP, and OCI
- Purchase with annual contracts or from the public cloud marketplaces



- Subscription based on data consumed and number of sites
- Hosted by Fortinet
- Delivered on AWS, Azure, GCP, and OCI
- CDN available at no additional cost
- Purchase with annual contracts or from the public cloud marketplaces
- Machine Learning threat detection
- Layer 7 DDoS protection
- FortiGuard antivirus, IP reputation, FortiSandbox Cloud, Credential Stuffing Defense, and WAF signatures
- Native HTTP/2 WAF protection
- REST API
- Advanced false positive mitigation
- Advanced SQLi detection
- API Discovery
- API Protection

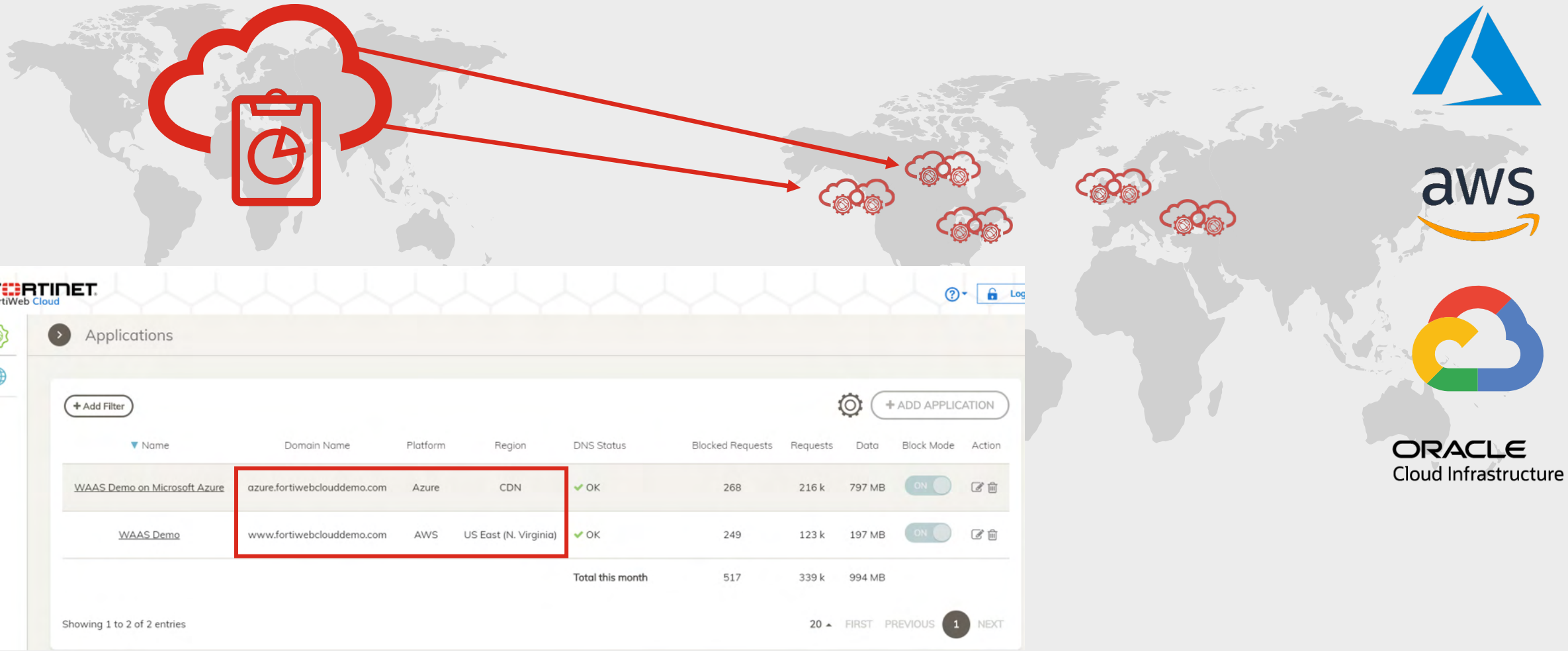
FortiWeb Cloud WAF as a Service

A cloud native web application and API protection solution

- Cloud Native
  - True multi-tenant SaaS solution, delivering elastic capacity
- Deployed in the same region as your application
  - Improved performance
  - Simplified regulatory environment
  - Reduce bandwidth costs
- Multi-Cloud
  - AWS
  - Azure
  - GCP
  - Oracle Cloud Infrastructure (OCI)

FortiWeb as a Service

Customer onboarding and provisioning



FortiWeb Cloud WAF as a Service—Global CDN

- Optional and available at no additional charge
- Directs requests to the nearest and fastest PoP
  - Latency based GSLB
- Worldwide distribution
  - Global distribution of WAF clusters
- Sophisticated caching and optimization techniques
  - Deliver content directly rather than forward to app

Purchasing Flexibility

Marketplace (Self-Service)

Fortinet FortiWeb Cloud WAF-as-a-Service	
Units	**Cost**
Hourly charge per web application protected by FortiWeb Cloud	$0.03 / unit
Total data transferred via FortiWeb Cloud (GB)	$0.4 / unit

Price + payment options	Billing term
$0.00/one-time payment Plus: Traffic: $0.40 gb Site Number: $0.03 one web site	1-month

Data Transferred	USD 0.40 /gibibyte
Web Application Protection	USD 0.03 /hour

Annual Subscription SKUs

SKU	Description
FC1-10-WBCLD-654-02-DD	FortiWeb Cloud WAF-as-a-Service—20Mbps average throughput—Annual Subscription. Select number of sites separately
FC2-10-WBCLD-654-02-DD	FortiWeb Cloud WAF-as-a-Service—50Mbps average throughput—Annual Subscription. Select number of sites separately
FC1-10-WBCLD-655-02-DD	FortiWeb Cloud WAF-as-a-Service—Additional 1 web site—Annual Subscription
FC2-10-WBCLD-655-02-DD	FortiWeb Cloud WAF-as-a-Service—Additional 5 web sites—Annual Subscription

Case Studies

Learn how Fortinet uses FortiWeb Cloud to protect our web applications

CASE STUDY

Fortinet Migrates Its Website to AWS, Protected by Its Own WAF-as-a-Service

Websites are the primary way that companies interact with their customers digitally, and global corporations typically have multiple web properties to support different business units, functions, and geographies. Fortinet is no exception, with a U.S.-focused primary website at www.fortinet.com, dozens of country-focused localized sites, and sites providing support, education, threat intelligence, and more.

"Deployment literally took just a few minutes, compared with anywhere from a half day to two days when we were testing the on-premises

CASE STUDY

Dynamic Cloud Security Enables Global Training & Enablement Group To Focus on Business Transformation

FORTINET

Fortinet is a Fortune 500 network security company that prides itself on leveraging technology to improve efficiency. An important team within the Fortinet Global Training & Enablement group, the systems development team designs, develops, and manages the custom web applications underlying Fortinet's award-winning training and certification programs. Like many lean teams with ambitious goals, the systems development team leverages a combination of off-the-shelf commercial and open-source solutions as building blocks. Using the open-source learning platform Moodle and the secure open web analytics platform Matomo for analytics, combined with three Atlassian commercial applications—Jira for project management, Bitbucket for version control, and Confluence for documentation—enables the team to focus on delivering cost-effective and highly scalable training applications.

"This application is absolutely critical to our business, so we decided to roll out FortiGate VM next-generation firewalls and FortiWeb web application firewalls. These enterprise security solutions alleviated


FORTINET